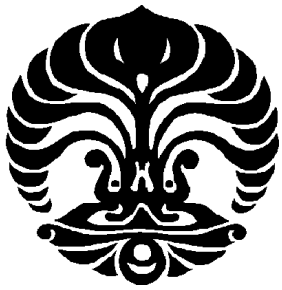
ASPEK HUKUM PROTOKOL PEMBAYARAN VISA/MASTERCARD SECURE ELECTRONIC TRANSACTION (SET)

Oleh:

Muhammad Aulia Adnan

Fakultas Hukum Universitas Indonesia



Depok, Jawa Barat
2000

DAFTAR ISI

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Internet, jaringan komputer terbesar di dunia pada saat ini digunakan oleh berjuta-juta orang yang tersebar di segara penjuru dunia. Internet membantu mereka sehingga dapat berinteraksi, berkomunikasi, belajar bahkan melakukan perdagangan dengan orang dari segala penjuru dunia dengan murah, cepat dan mudah. Penggunaan internet untuk berbagai macam kegiatan ini sudah berbeda jauh dengan tujuan semula adanya jaringan ini. Internet pada mulanya adalah suatu penelitian yang dilakukan oleh *Advanced Research Projects Agency* (ARPA)[1] suatu bagian dari *US Department of Defense*. Jaringan ini akan berfungsi sebagai alat komunikasi yang akan menghubungkan pihak militer, universitas dan para produsen peralatan militer. Internet akan menjadi suatu jaringan infrastruktur komunikasi alternatif apabila jaringan utamanya hancur dalam suatu serangan nuklir[2].

Teknologi internet mempunyai pengaruh yang sangat besar terhadap perekonomian dunia. Internet membawa perekonomian dunia memasuki babak baru yang lebih populer dengan istilah *digital economics* atau perekonomian digital. Makin banyak kegiatan perekonomian dilakukan melalui media internet. Perdagangan, misalnya, semakin banyak mengandalkan *e-commerce* sebagai media transaksi.

---

[1] Joseph Ruh Jr., ed., *The Internet and Business: a Lawyers Guide to the Emerging Legal Issues*, (Computer law association,1996)

[2] Jaringan internet dibuat pada saat perang dingin (*cold war*), sehingga pihak militer merasa perlu membuat suatu jaringan komunikasi alternatif apabila terjadi serangan nuklir yang menghancurkan sarana komunikasi.

Internet telah berkembang sedemekian pesat terutama pengaruhnya terhadap dunia binis. Presiden Amerika Serikat, Bill Clinton mencermati perkembangan internet, sebagai berikut:

> *No single force embodies our electronic transformation more than evolving medium known as the internet Entrepreneurs are able to start new business more easily, with smaller up-front investment requirements, by accessing the internet's world wide network of customer*[3].

E-commerce pada dasarnya adalah merupakan suatu kontak transaksi perdagangan antara penjual dan pembeli dengan menggunakan media internet. Jadi, proses pemesanan barang, pembayaran transaksi hingga pengiriman barang dikomunikasikan melalui internet.

Dilihat dari jenis transaksinya , *e-commerce* dikelompokan menjadi dua segmen yaitu, *business to business e-commerce* (B2B *e-commerce*) dan *business to consumer* (B2C). B2B e-commerce adalah transaksi perdagangan melalui internet, yang dilakukan oleh dua atau lebih perusahaan. Transaksi ini biasanya dilakukan untuk pembelian bahan baku atau komponen pendukung kegiatan produksi ataupun perdagangan. Dalam dunia bisnis, transaksi dagang tersebut sering disebut sebagai *Enterprise Resources Planning*.(ERP) ataupun *supply chain management*. Sedangkan B2C *e-commerce* merupakan transaksi jual beli melalui internet antara penjual barang konsumsi dengan konsumen (*end user*).

Penggunaan internet sebagai media perdagangan terus meningkat dari tahun ke tahun, hal ini disebabkan karena berbagai manfaat yang didapat oleh perusahaan ataupun konsumen dengan melakukan transaksi melalui internet. Nilai perdagangan dunia dengan menggunakan media internet (hanya untuk B2C *e-commerce*) adalah sebagai berikut:

---

[3]William J. Clinton, *A Framework for Global Electronic Commerce*, Washington, D.C.<http://www.white_house.gov>

Tabel 1

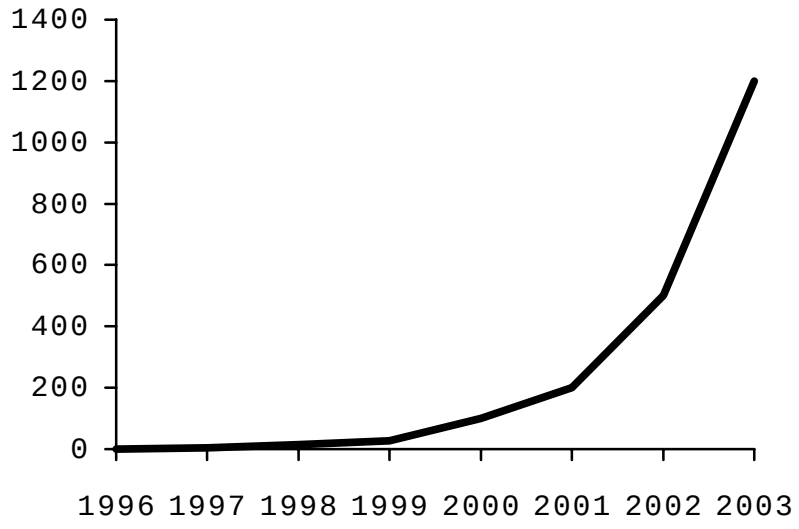
Sumber	**1996** *(dalam jutaan US $)*	**2000** *(dalam jutaan US $)*
Yankee Group	750	10,000
Jupiter	1200	7300
Forrester Research	530	7170

Sumber: eMarketer

Transaksi *e-commerce* di Indonesia sendiri menunjukan trend yang akan terus naik dengan pesat. Nilai transaksi tersebut mencapai US$100 juta pada tahun 2000 dan akan naik menjadi US$ 200 juta pada tahun 2001

Gambar 1

(dalam jutaan US $)



Sumber: *International Data Corporation* (IDC 99)

Berdasarkan data tersebut diatas maka dapatlah disimpulkan bahwa nilai transaksi *e-commerce* adalah sangat kecil dibandingkan nilai transaksi didunia. Rendahnya nilai transaksi di Indonesia bukanlah disebabkan oleh rendahnya faktor permintaan (*demand*) tetapi karena ketidaksiapan infrastruktur pendukung[4]. Infrastruktur ini antara lain adalah *Payment Gateway*, Lembaga Sertifikasi(*Certification Authority*) dan aturan hukum yang mengatur masalah transaksi elektronis.

Besarnya nilai transaksi e-commerce di dunia masih dibayangi masalah "kurang amannya(*secure*)" transaksi on-line ini. Internet telah menimbulkan berbagai masalah terutama yang berkaitan dengan masalah kerahasian, keutuhan pesan *(integrity*), identitas para pihak dan hukum yang mengatur transaksi tersebut. Permasalahan-permasalahan tersebut kemudian kemudian coba dipecahkan dengan menggunakan teknik kriptografi[5]. Teknik kriptografi banyak membantu kita dalam hal keamanan (*security*), keutuhan pesan (*integrity*), dan juga masalah identitas dari para para pihak. Meskipun secara teknis masalah-masalah yang berkaitan dengan transaksi secara on-line dapat dipecahakan tetapi secara yuridis/hukum hal ini akan menimbulkan berbagai permasalahan. Sistem hukum kita (juga dunia) secara umum belum mengenal atau tidak mengatur secara khusus pengunaan teknik kriptografi dalam suatu kontrak.

Berbagai lembaga internasional berusaha untuk mengatasi hal ini dengan dengan memberikan panduan bagi para pihak (individu atau negara) dalam mengatasi masalah penggunaan teknik kriptografi secara yuridis. Panduan ini bisa berupa *guidelines* ataupun *model law*. Terdapat beberapa lembaga internasional yang mengeluarkan panduan antara lain; OECD[6], ICC[7], ISETO[8] dan Uncitral[9] .

---

[4] "Era ekonomi digital telah tiba", *Bisnis Indonesia* (29 Juni 1999): 1.

[5] Pembahasan lebih lanjut mengenai kriptografi akan dijelaskan dalam bab 2 .

[6] OECD, Report on Global Information Infrastructure-Global Information Society, Cryptography Policy Guidelines and the report on Background Issues of Cryptography Policy, <http://www.oecd.org/dsti/sti/it/secur/prod/GD97-204.htm>

[7] ICC (International Chamber of Commerce), General Usage for International Digitally Ensured Commerce (GUIDEC), <http://www.iccwbo.org>

Infrastruktur pendukung dari *e-commerce* salah satunya adalah adanya suatu sistem pembayaran berbasis internet (*Internet Payment System*) dalam hal ini adalah SET (*Secure Electronic Transaction*). SET adalah suatu sistem pembayaran yang dipelopori oleh Mastercard dan Visa International[10]. Sistem pembayaran ini menggunakan kriptografi dalam pelaksanaanya, sehingga dapat menjamin keamanan transaksi ini. SET didukung oleh berbagai vendor dunia yang bergerak dalam bidang transaksi internet yang aman (*internet secure transaction*) antara lain adalah GTE Cybertrust, IBM, Netscape, SAIC, Terisa system dan juga Verisign Inc[11].

Ketiadaan infrastruktur (baik teknis ataupun hukum) khususnya dalam sistem pembayaran (*internet payment system*) merupakan penghambat bagi perkembangan *e-commerce* di Indonesia. Keberadaan suatu kajian terhadap *internet payment System* terutama aspek yuridis dari penggunaan teknik kriptografi diharapkan dapat menambah wacana pengetahuan dalam mendorong perkembangan *electronic commerce* di Indonesia.

---

[8] ISETO (International Secure Electronic Transaction Organization), suatu organisasi internasional yang berkedudukan di Swiss berusaha menciptakan infrastruktur yang akan menjamin keamanan dalam melakukan transaksi di internet.), <http://www.iseto.ch>

[9] Uncitral, model law on e-commerce, General Assembly resolution 51/162 of 16 December 1996

[10] Mastercard dan Visa International, *SET Secure Electronic Transaction Specification Book 1*: *Business Description* (versi 1,1997), hal.1

[11] Lary Loeb, "the Stage is Set," *The Internet World* (Agustus 1996)

B. PERMASALAHAN

1. Ruang Lingkup Permasalahan

Bank dalam menjalankan fungsinya sebagai lembaga keuangan antara (*financial intermediary*) memberikan berbagai macam jasa, antara lain adalah jasa pembayaran (*payment*). Jasa pembayaran pada saat ini berkembang pesat kearah *electronic/internet payment system*. *Internet Payment System* ini menimbulkan berbagai permasalahan dari segi teknis maupun dari segi hukum. Permasalahan ini secara umum adalah masalah yang berhubungan dengan keamanan, identitas/otentisitas dari para pihak dan masalah kontrak. Secara teknis permasalahan ini coba dipecahkan dengan menggunakan teknik kriptografi. SET sebagai salah satu bentuk *Internet Payment System* menggunakan teknik ini untuk menjamin keamanan transaksi pembayaran ini. Meskipun secara teknis sistem pembayaran in adalah aman tetapi secara hukum hal ini menimbulkan berbagai permasalahan. Dalam skripsi ini penulis membatasi ruang lingkup permasalahan pada tinjauan yuridis terhadap SET (*Secure Electronic Transaction*) berdasarkan hukum yang berlaku di Indonesia dan juga aturan yang berlaku secara internasional. Aturan yang berlaku secara internasional ini bisa berupa panduan (*guidelines*), model aturan (*model law*) dan juga bentuk-bentuk lainnya. Tinjauan yuridis ini terutama adalah implikasi penggunaan teknik kriptografi dalam suatu transaksi dengan menggunakan media internet (dalam hal ini SET).

2. Perumusan Pokok-pokok Permasalahan

Berdasarkan latar belakang masalah dan ruang lingkup permasalahan, penulis merumuskan pokok-pokok permasalahan sebagai berikut:

1. Apakah *Internet Payment System* itu, terutama skim (*scheme*) dari *Secure Electronic Transaction* (SET)?

2. Bagaimanakah standar keamanan dari SET dan bagaimanakah skim ini menentukan para pihak (subyek hukum), hubungan hukum dan kontrak?
3. Bagaimanakah *Uncitral model law on electronic commerce* mengatur tentang transaksi dengan menggunakan media internet (dalam hubungannya dengan SET) ? .
4. Bagaimanakah aturan hukum di Indonesia mengatur hal ini?
5. Permasalahan hukum apa saja yang muncul sehubungan dengan adanya *Payment instruction* berbasis SET ?

C. TUJUAN PENULISAN

Dalam melakukan pembahasan permasalahan yang sesuai dengan judul skripsi, penulis mempunyai beberapa tujuan yang diharapkan dapat dicapai melalui pembahasan dalam skripsi ini.

Meningkatnya nilai transaksi yang terjadi melalui media *e-commerce*, menimbulkan adanya kebutuhan akan adanya suatu transaksi pembayaran yang aman. Kriteria dari aman disini adalah aman baik secara teknis maupun secara yuridis. Secara teknis hal ini dapat dapat dicapai dengan digunakannya teknik kriptografi. Sedangkan secara yuridis adalah dengan adanya suatu perangkat perundang-undangan yang mengatur tentang penggunaan teknik kriptografi dalam suatu hubungan hukum (kontrak). Dalam skripsi ini penulis hendak mengetahui apakah *Internet Payment System* itu terutama mengenai SET.

Skim SET menggunakan *digital signature* sebagai bentuk kontrak diantara para pihaknya. Penggunaan *digital signature* sebagai suatu bentuk kontrak akan menimbulkan berbagai implikasi hukum. Penulis ingin mengetahui bagaimanakah penerapan dan implikasi hukum dari penggunaan *digital signature* dalam suatu kontrak.

Penerapan teknik kriptografi dalam transaksi dengan menggunakan *e-commerce* telah menimbulkan berbagai implikasi hukum yang rumit. Hal ini terutama karena terdapat berbagai macam metode kriptografi yang dipergunakan dalam suatu transaksi. Uncitral, sebagai suatu badan PBB yang menangani masalah perdagangan internasional

berusaha mengatasi kerumitan-kerumitan tersebut dengan membuat suatu model hukum/perundang-undangan (*model law*), yaitu *Uncitral Model Law on electronic commerce*. Penulis ingin mengetahui bagaimanakah *model law* ini menagtur mengenai penggunaan *digital signature* dalam skim SET.

Mengingat perlu adanya suatu perlindungan hukum bagi warganegara Indonesia yang menggunakan metode SET ini, maka perlu adanya suatu perundang-undangan yang mengatur penggunaan teknik kriptografi dalam suatu kontrak. Penulis ingin mengetahui apakah terdapat peraturan di Indonesia yang mengatur hal ini, jika tidak ada maka penulis hendak mengetahui bagaimanakah sebaiknya aturan tersebut.

Penggunaan internet dan juga sistem pembayaran di internet (SET) telah menimbulkan berbagai permasalahan hukum. Penulis ingin mengetahaui apakah permasalahan hukum yang timbul sehubungan dengan dipakainya sistem pembayaran berbasis SET dalam *e-commerce*.

D. METODE PENELITIAN

Metodologi penelitian yang digunakan oleh penulis dalam penulisan ini adalah sebagai berikut:

1. Jenis Penelitian

Penelitian ini bersifat deskriptif analitis, yakni pada awalnya bersifat menggambarkan situasi yang ada yaitu penggunaan teknik kriptografi dalam pengamanan dalam suatu transaksi *on-line*. Teknik ini juga digunakan dalam skim (*scheme*) SET yang akan melindungi para pihak dalam melakukan transaksinya. Kemudian berdasarkan data-data ini kemudian akan dilakukan analisis berdasarkan data yang telah ada dan kemudian menghubungkan dengan teori-teori yang ada hubungannya dengan tema skripsi ini.

2. Teknik Pengumpulan Data

Dalam penulisan ini penulis dalam pengumpulan datanya menggunakan teknik:

a. Metode penelitian literatur (*library research*), yaitu penelitian kepustakaan dengan menggunakan bahan-bahan pustaka hukum yang mendukung. Bahan pustaka yang dipakai dibedakan menjadi:

1. Bahan hukum primer, yaitu bahan yang mempunyai kekuatan mengikat yang mengikat seperti norma dasar, peraturan perundang-undangan atau keputusan pengadilan. Dalam penelitian menggunakan bahan hukum primer yang berupa peraturan perundang-undangan dan norma hukum.
2. Bahan hukum sekunder, yaitu bahan hukum yang memberi penjelasan mengenai bahan hukum primer. Bahan hukum sekunder yang dimaksud disini adalah bahan hukum yang menjelaskan bahan hukum primer dan isinya tidak mengikat. Bahan hukum sekunder yang digunakan penulis disini adalah buku yang membahas mengenai masalah penggunaan teknik kriptografi dalam suatu pesan (*messages*), penulis juga menggunakan bahan-bahan yang terdapat dalam mengenai sistem pembayaran, sistem keamanan dan implikasi hukum dari sistem pembayaran berbasis internet.
3. Bahan hukum tertier, yaitu bahan hukum yang memberi petunjuk maupun penjelasan terhadap bahan hukum primer maupun sekunder. Dalam kajian ini, dipakai kamus dan ensiklopedi yang berkaitan dengan masalah yang dikaji.

b. Penelitian Lapangan (*field research*), selain penelitian kepustakaan, penulis juga akan mengadakan penelitian lapangan dengan cara mengadakan wawancara. Dalam penulisan skripsi ini, penulis akan melakukan penelitian lapangan dengan mengajukan pertanyaan langsung kepada informan atau para praktisi dalam bidang internet dan sistem keamanannya.

E. SISTEMATIKA PENULISAN

Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

Bab I : Bab ini merupakan bagian pendahuluan penulisan, yaitu terdiri dari latar belakang, ruang lingkup permasalahan, metode penelitian, dan sistematika penulisan.

Bab II : Bab ini akan menerangkan tentang sejarah internet, protokol yang dipergunakan, kriptografi, beberapa bentuk sistem pembayaran berbasis internet (*internet payment system*), termasuk didalamnya *Secure Electronic Transaction* (SET).

Bab III Bab ini akan menerangkan berbagai permasalahan hukum yang berhubungan dengan transaksi pembayaran berbasis SET. Permasalahan mengenai identitas para pihak, hubungan hukum antara para pihak, keabsahan kontrak pembayaran elektronis secara yuridis.

Bab IV Bab ini akan berisi kesimpulan dari pembahasan bab-bab sebelumnya dan juga berisi saran-saran dari hasil kesimpulan.

BAB II

TINJAUAN UMUM TERHADAP SISTEM PEMBAYARAN BERBASIS SET (*Secure Electronic Transaction*) DALAM E-COMMERCE

A. INTERNET

Internet sebagai suatu bentuk jaringan komputer mempunyai beberapa keunikan yang tidak dipunyai oleh suatu bentuk jaringan komputer yang lain yang ada pada saat ini. Internet terdiri dari suatu kelompok jaringan (yang terus tumbuh) yang terdiri baik jaringan publik maupun jaringan privat, *Local Area Networks* (LANs), *Wide Area Networks* (WANs) yang satu sama lain saling terhubung (*interconnect*). Secara teknis internet adalah " *a network of many networks, all running the TCP/IP protocol suite…, connected through gateways, and sharing common name and address spaces*"[12]. Adanya interkoneksi dengan berbagai jaringan inilah yang menyebabkan internet berbeda dengan jaringan yang ada lainnya. Interkoneksi inilah yang menghubungkan setiap orang dimanapun ia berada di dunia ini dapat mengakses internet baik melalui jaringan lokal, regional ataupun internasional sehingga ia dapat berkomunikasi dengan orang lain dimanapun orang itu berada.

Jaringan-jaringan (*networks*) yang saling terhubung itu, berkomunikasi satu sama lainnya dengan suatu teknologi komunikasi yang terdiri dari suatu kelompok protokol[13]

---

[12] J. Quatermar, *The Matrix: Computer Networks and Confrencing Systems Worldwide* (1990)

[13] Protokol secara singkat adalah sekumpulan aturan dan spesifikasi mengenai suatu cara komunikasi. Setiap protokol mempunyai aturan tersendiri, sehingga ia dapat melakukan suatu fungsi dalam berkomunikasi. Sejak pertama kali diciptakan TCP/IP adalah suatu protokol yang terbuka (*open protocol*), sehingga setiap orang dapat membuat suatu protokol sendiri yang dapat dijalankan dalam suatu sistem. Hal ini menyebabkan

yang secara singkat disebut dengan TCP/IP (*Transfer Control Protocol/Internet Protocol*).

TCP/IP pertamakali dikembangkan oleh *US Department of Defense*, maksud dari pengembangannya adalah untuk membuat suatu jaringan komputer militer yang dapat tetap terhubung satu sama lainnya meskipun terdapat salah satu komponennya rusak dalam suatu serangan militer[14]. TCP/IP berfungsi untuk membagi-bagi data digital menjadi paket-paket kecil (*datagram*) yang kemudian akan ditransmisikan melalui melalui jaringan ke suatu tujuan yang dikehendaki. Rute maupun jenis jaringan/perangkat jaringan yang akan dilewati oleh data tersebut adalah tidak penting. Masing-masing paket data tersebut dapat melalui rute yang berbeda satu sama lainnya. Jika kita mengirim suatu surat/pesan melalui internet, TCP akan membagi pesan kedalam peket-paket data yang kecil. Setiap paket data tersebut akan ditandai dengan nomer urut dan alamat penerima. Selain itu TCP akan menyertakan informasi untuk mengontrol jika terjadi kesalahan.

Paket-paket data tersebut dikirim melalui jaringan komputer, dimana dalam tahap ini IP membawa paket-paket data tersebut dan memeriksanya jika terjadi kesalahan. Setelah semua paket data itu dapat diterima secara benar, TCP menggunakan nomer urut tersebut untuk merekonstruksi pesan asli. Berdasarkan uraian tersebut maka fungsi dari TCP adalah mengatur paket-paket data dan memastikan kebenaran paket data. Sedangkan fungsi dari IP adalah membawa paket-paket data dari suatu tempat ke tempat yang lainnya.

Internet menghubungkan (*Interconnect*) berbagai jaringan yang ada di dunia. Kemampuan ini menjadikan internet sebagai suatu jaringan publik yang mempunyai

---

berbagai sistem yang berbeda dapat saling berkomunikasi dan terhubung satu sama lainnya. Hal inilah salah satu alasan mengapa perkembangan internet sangat cepat.

[14] L.J. Davies, *The Internet and The Elephant*, (Center of Commercial Law Studies, 1995) <http: www.ccls.edu/itlaw/publications/html/inetiba.html>

sifat terbuka (*Open & Public Network*). Jaringan terbuka (*open network*) ini mempunyai berbagai keuntungan dibandingkan jaringan yang tertutup (*closed network*), misalnya kemudahan dalam mengakses jaringan dengan biaya infrastruktur jaringan yang kecil. Kelebihan dari *open network* ini dibarengi pula dengan meningkatnya resiko terhadap jaringan ini yaitu resiko mengenai keamanan (*security*). Kriteria "terbuka" terhadap jaringan internet ini oleh *The National Research Council* diartikan sebagai berikut[15]:

1. Terbuka/bebas digunakan oleh setiap pengguna (*users*), hal ini disebabkan tidak adanya paksaan untuk menjadikan seseorang untuk menjadi anggota kelompok tertentu agar ia dapat mengakses internet. Internet tidak membatasinya seseorang untuk mengakses jaringannya.
2. Terbuka terhadap setiap penyedia jasa layanan (*service providers*). Adanya keterbukaan terhadap setiap jenis layanan ini akan menimbulkan iklim persaingan yang sehat dimana setiap penyedia jasa layanan dapat berkompetisi secara sehat.
3. Terbuka terhadap kemungkinan perubahan, hal ini dikarenakan internet selalu memperkenankan adanya suatu perubahan/penemuan baru dalam bidang-bidang aplikasi dan jasa. Internet memperkenankan adanya teknologi baru untuk dipakai oleh publik (masyarakat).

B. FASILITAS PADA INTERNET

Internet sebagai suatu jaringan komputer mempunyai berbagai kemampuan atau fasilitas bagi para penggunanya. Para pengguna internet dari segala penjuru dunia dapat saling berkomunikasi satu sama lain dengan mempergunakan fasilitas yang ada di internet. Fasilitas tersebut antara lain, adalah:

---

[15] National Research Council, *Realizing the Information Future: the Internet and Beyond*, (The National research council,1994) hal:44

1. *E-mail*

Fasilitas ini merupakan fasilitas dari internet yang paling banyak digunakan. Setiap pemakai internet dapat mengirim dan menerima pesan dari orang lain yang juga terhubung dengan internet. Pesan yang dikirim oleh orang tersebut akan diterima oleh penerimanya hampir secara seketika. Keunggulan dari fasilitas ini adalah biaya yang harus dikeluarkan oleh seseorang dalam mengirim maupun menerima suatu *e-mail* adalah hampir tidak ada.

2. *File Transfer Protocol (FTP)*

FTP adalah suatu protokol dasar yang menyediakan kemampuan untuk mentransmisikan *file* dari satu komputer ke komputer yang lain atau dari satu *server* ke *client*.

3. Real Time Communication (CHAT)

Fasilitas ini berbeda dengan *e-mail* dalam hal pesan yang dikirim oleh pengirim dapat dilihat oleh penerima secara seketika. Penerima kemudian, dapat dengan segera membalasnya (*reply*) dan pengirim (yang pertama) dapat pula dengan segera membalas *reply* ini.

4. *World Wide Web (WWW)/ Web*

World Wide Web merupakan fasilitas di internet yang dikembangkan pada awal 1990 di CERN (*European Laboratory for Particle Physics*)[16]. *Web* adalah fasilitas di

[16] Joseph F. Ruh Jr., "Introduction to the internet" dalam *The Internet and Business: A Lawyers Guide to the Emerging Legal Issues*, (Computer Law Association:1996)

internet yang sangat memudahkan para pengguna internet berpindah (*jump*) dari satu halaman *web* ke halaman *web* yang lain. *Web* menggunakan suatu protokol tertentu yaitu HTTP (*Hypertext Transfer Protocol*) untuk mentransmisikan dokumen-dokumen yang dibuat dalam format *Hypertext Markup Language* (HTML) dari *server* ke *client*. *Hypertext* adalah suatu ide mengenai bagaimana menghubungkan suatu informasi dengan informasi yang lain sehingga informasi tersebut dapat diakses, hal ini berbeda dengan membaca informasi tersebut secara berurutan (*sequential*). Dengan mempergunakan *mouse* untuk mengklik suatu *hypertext link*, seorang pengguna dapat berpindah (*jump*) ke suatu informasi lain (yang masih ada hubungannya dengan informasi yang pertama).

C. PENGUNAAN INTERNET UNTUK BISNIS

Perkembangan internet adalah sangat fenomenal, hal ini dapat dilihat dari banyaknya orang yang menggunakannya, besarnya nilai bisnis yang ada, berbagai macam barang atau jasa yang ditawarkan melaluinya. Internet telah mengubah cara orang melakukan komunikasi (*e-mail, chat, internet phone*), belajar (*distance learning with video confrencing*), berbelanja (*cyberstore/e-commerce*). Internet menciptakan berbagai macam bidang usaha yang baru yang sebelumnya tidak pernah ada. Internet telah membuka batas-batas antar negara sehingga teknologi ini membawa kita semakin dekat ke dalam era globalisasi. Jika kita berbicara pasar didalam *e-commerce* maka tentulah pasar (*market*) yang dimaksud adalah pasar dunia dan bukan menunjuk secara spesifik suatu daerah tertentu saja. Para pihak yang terlibat dalam pasar ini tidak hanya para penjual dan pembeli, tetapi didalamnya terlibat pula lembaga keuangan sebagai penyedia jasa layanan pembayaran yang dapat dilakukan dengan seketika (*real time*) secara *on-line*.

Kemungkinan melakukan bisnis yang sangat luas melalui internet yang lebih dikenal dengan sebutan *electronic commerce* (*e-commerce*) menyulitkan kita untuk

mengetahui apakah ruang lingkup dari *commerce* tersebut. Uncitral dalam *Model Law on electronic commerce* mendefinisikan *commerce* sebagai:

> "The term 'commercial' should be given a interpretation so as to cover matters arising from all relationship of a commercial nature whethere contractual or not. Relationship of a commercial nature include but are not limited to the following transactions for the supply or exchange of goods or services; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concesion; carriage of goods or passenger by air, sea, rail or road[17]"

Melihat dari definisi diatas maka dapat kita lihat bahwa *e-commerce* membuka banyak sekali peluang bisnis. Peluang bisnis ini meliputi barang maupun jasa. Barang disini bisa berupa barang yang kita kenal selama ini ataupun dalam bentuk digital.

Perkembangan *e-commerce* ini membutuhkan berbagai infrastruktur untuk menunjang perkembangannya. Salah satu infrastruktur yang sangat penting adalah adanya layanan pembayaran secara *on-line* yang aman. Adanya jaminan kepastian dalam pembayaran dan juga keamanan dalam sistem pembayaran inilah salah satu penyebab mengapa terdapat keenganan seseorang melakukan transaksi via internet.

Kalangan bisnis melihat *e-commerce* adalah sebagai suatu kemungkinan bisnis yang baru dengan banyak sekali keunggulan yang dipunyainya. Berbagai keunggulan itu antara lain:

1. Jangkauan/cakupan yang luas dan basis konsumen yang besar. Para pengecer yang menggunakan *web* akan menikmati keuntungan dari jumlah konsumen yang

---

[17] Uncitral, Uncitral model Law on Electronic commerce with guide to enacment 1996 with additional article 5 bis as adopted in 1998, general assembly resolution 51/162 of 16 December 1996

terus bertambah banyak. Berbagai hambatan geografis yang ada selama ini menjadi hilang dan tidak ada batasan mengenai jangka waktu kegiatan. Jam beroperasi hanya dibatasi oleh *hardware* dan *software* yang digunakan.

2. Pendapatan yang terus bertambah. *Web* membuka berbagai kemungkinan dalam melakukan penjualan dan distribusi. *Merchants* mendapatkan berbagai keuntungan dari besarnya pasar yang ada baik dilihat secara geografis maupun dilihat dari sisi jumlah konsumen.
3. Penghematan biaya. Penggunaan *e-commerce* akan dapat secara drastis mengurangi biaya inventaris/persediaan yang harus disediakan oleh *merchant* dalam suatu waktu. Terdapat berbagai perusahaan yang tidak mempunyai persediaan (*inventory*) tetapi mereka dapat menawarkan berbagai macam produk kepada pelanggannya. Mereka hanya menghubungkan antara berbagai macam permintaan yang ada kedalam sistem yang digunakan oleh produsen.
4. Hubungan yang lebih baik dengan konsumen. Perdagangan secara *on-line* mempunyai kemampuan untuk berinteraksi dengan konsumen secara lebih dekat dan cepat. Konsep ini dikenal sebagai *one to one marketing*[18], dimana *merchant* dapat secara langsung berinteraksi dengan konsumen.

Perkembangan internet dan *e-commerce* yang sangat pesat dan disertai dengan berbagai kemungkinan bisnis yang ada, ternyata mempunyai beberapa kelemahan. Kelemahan ini terutama menyangkut masalah keamanan dan perlindungan hukum bagi para pihak yang terlibat. Sebagai jaringan publik yang terbuka (*open network*), internet rentan terhadap berbagai macam kejahatan misalnya adanya kemungkinan dicurinya nomor kartu kredit atau dipergunakan oleh orang lain. Hal ini menyebabkan adanya kalangan yang masih takut untuk membayar suatu barang/jasa via internet dengan alasan

---

[18] Seth Godin, *Presenting Digital Cash Learn How Cash Will Affect How we Spend*, (Indiana: Sams.net Publishing 1995), hal. 35

keamanan. Selain itu juga adanya masalah yang berkaitan dengan perlindungan hukum bagi para pihak, misalnya masalah kontrak jual beli yang dilakukan bukan diatas kertas (*paper based*).

Berbagai kelemahan tersebut diatas coba diatasi dengan menggunakan teknologi penyandian informasi(*cryptography*). *Electronic data transmission* dalam *e-commerce* dilindungi dengan melakukan proses enkripsi (*encrypt*) dengan menggunakan suatu algoritma sehingga menjadi *cipher/locked data* yang hanya dapat dibaca dengan melakukan proses *reversal* yaitu proses *decrypt*. Selain sistem keamanan diatas dapat juga diterapkan sistem pengamanan yang lain seperti *firewall*, *smartcard* dan juga penerapan *System Operating Procedures* (SOP) yang kuat[19]. Penggunaan tehnik kriptografi ini juga akan menimbulkan suatu produk perundang-undangan baru yang mengaturnya yang biasanya disebut dengan *Digital Signature Act, Electronic Signature Act*. *Uncitral* mengatur hal ini dalam *Model Law on e-commerce.* Didalam skripsi ini masalah keamanan yang hendak dibahas adalah masalah hukum yang berhubungan dengan sistem keamanan dalam transaksi pembayaran berbasis SET.

D. KRIPTOGRAFI (CRYPTOGRAPHY)

Kriptografi adalah seni dan ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim (*originator*) dapat disampaikan kepada penerima (*receiver*) dengan aman[20]. Kriptografi juga dapat diartikan sebagai suatu bidang ilmu pengetahuan yang mempelajari teknik-teknik aplikasi yang keberadaanya tergantung pada keberadaan suatu masalah yang sukar atau sulit[21]. Didalam kriptografi dikenal

---

[19] SOP adalah prosedur baku dalam melakukan pekerjaan tertentu di pabrik atau kantor.

[20] Bruce Schneir, *Applied Crypthography*, 2nd ed.,(NewYork:John Willey and Sons Inc., 1996) hal.1

berbagai macam istilah misalnya *Cryptanalysis* yaitu ilmu pengetahuan yang mempelajari bagaimana mengetahui (*compromise/defeat*) mekanisme kriptografi. *Cryptology* (berasal dari bahasa Yunani, *krypto* dan *logos*) yang berarti *hidden world* adalah suatu bidang yang mengkombinasikan *Crythography* dan *Crypthoanalysis*[22].

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

1. *Confidentiality* (kerahasiaan); suatu pesan tidak boleh dapat dibaca atau diketahui oleh orang yang tidak berkepentingan.
2. *Authenticity* (otentisitas); penerima pesan harus mengetahui atau mempunyai kepastian siapa pengirim pesan dan bahwa benar pesan itu dikirim oleh pengirim. Istilah ini juga berhubungan dengan suatu proses verifikasi terhadap identitas seseorang.
3. *Integrity* (integritas/keutuhan); penerima harus merasa yakin bahwa pesan yang diterimanya tidak pernah diubah sejak pesan itu dikirim hingga diterima, seorang pengacau tidak dapat mengubah atau menukar isi pesan yang asli dengan yang palsu.
4. *Non repudiation* (tidak dapat disangkal); pengirim pesan tidak dapat menyangkal bahwa ia tidak pernah mengirim pesan tersebut.

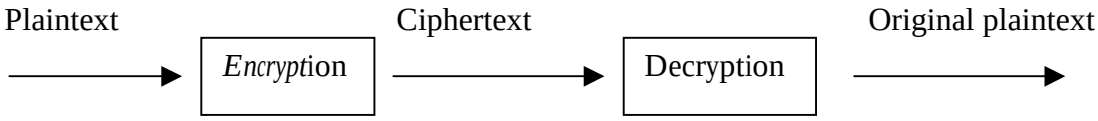
Penggunan kriptografi dalam *e-commerce* (internet) telah banyak membantu dalam menyelesaikan masalah keamanan (*security*) dan juga masalah hukum. Kriptografi memungkinkan terciptanya suatu sistem komputer yang terpercaya (*trustworthy computer system*).

---

[21] RSA Laboratories, *Frequently Asked Question about Today's Crypthography 4.0* (RSA Data Security Inc., 1998), p.2

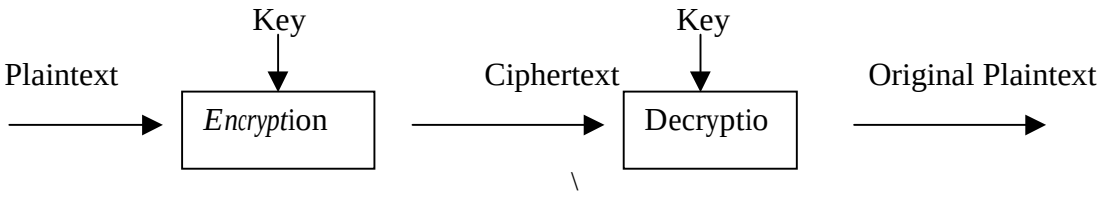
[22] Schneir, *op.cit*..hal. 2

Pesan (*messages*) asli dalam kriptografi biasanya disebut *Plaintext. Plaintext* bisa terdiri dari suatu *text file*, *bitmap*, *digitized voice*, *digital video image* dan lain sebagainya. *Encryption* adalah proses transformasi suatu pesan/data menjadi suatu bentuk yang hampir mustahil untuk dibaca tanpa adanya suatu pengetahuan yang sesuai mengenai algoritma (*key*) pesan yang sudah ditransformasikan tersebut disebut dengan *ciphertext*. Proses pengembalian (*recovery*) dari *ciphertext* ke pesan yang semula disebut dengan proses dekripsi (*decrypt*).



GAMBAR 2.1. PROSES ENCRYPTION DAN DECRYTION

Kriptografi modern pada saat ini menggunakan "kunci" (*key*). Kunci ini menggantikan fungsi algoritma dalam proses *encryption*. Penggunaan kunci ini mempunyai berbagai kelebihan antara lain mudah didistribusikan secara meluas, sehingga banyak digunakan pada saat ini.



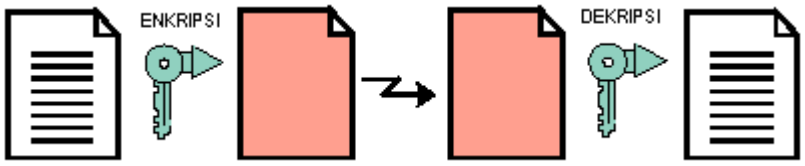
GAMBAR 2.2. ENCRYPTION DAN DECRYPTION DENGAN MENGGUNAKAN KEY

1. *Algoritma Simetris (Symmetric Algorithm)*

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

algoritma yang sering digunakan, sehingga seringkali disebut sebagai dengan algoritma konvensional. Didalam kebanyakan algoritma simetris kunci yang digunakan untuk melakukan *encryption* adalah sama dengan yang digunakan untuk melakukan *decryption*. Algoritima ini sering juga disebut sebagai *secret-key algorithm, single-key algorithm, one-key algorithm* atau *symmetric key*[23].

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



GAMBAR 2.3. ENKRIPSI DAN DEKRIPSI PADA SEBUAH DOKUMEN

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

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

1. Pengirim dan penerima menggunakan kunci yang sama, sehingga mereka masing-masing haruslah mempunyai kunci yang sama agar mereka dapat

---

[23] Schneir,Ibid., hal.4

melakukan komunikasi. Mereka harus saling percaya bahwa tidak akan memberikan kunci tersebut kepada orang lain.

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

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

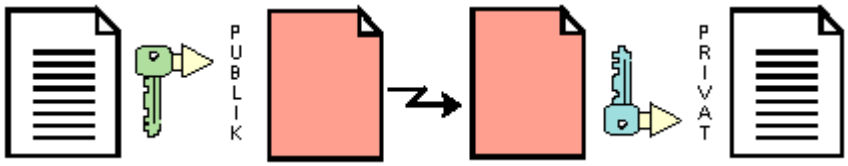
2. *Algoritma kunci public (Public-Key Algorithm)*

Public-key Algorithm sering juga disebut sebagai algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda antara kunci yang digunakan untuk melakukan enkripsi dan yang digunakan untuk melakukan dekripsi. Kunci tersebut dinamakan kunci privat (*privat key*) dan kunci publik (*public key*).

Algoritma ini dinamakan dengan algoritma kunci publik karena kunci yang akan digunakan untuk melakukan *encryption* (kunci publik) adalah dapat didistribusikan ke umum (publik). Seseorang yang tidak dikenal dapat saja menggunakan kunci tersebut untuk meng-*encrypt* suatu pesan, tetapi hanya orang tertentu saja (yaitu yang mempunyai kunci privat) yang dapat membuka pesan tersebut (mendenkrip). Kedua kunci tersebut (kunci privat dan kunci publik) mempunyai hubungan secara matematis, meskipun demikian seseorang yang mempunyai kunci publik tidaklah dapat membuat kunci privat dari kunci publik tersebut[24].

---

[24] Schneir, *ibid*., hal 5

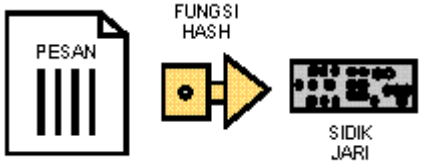


Gambar 2.4. Enkripsi dan Dekripsi pada *Asymmetric Algorithm*

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

3. *Fungsi Hash (*Hash function*)*

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



GAMBAR 2.5. FUNGSI HASH

4. *Digital Signature*

Digital signature dapat dihasilkan baik dengan menggunakan algoritma simetris ataupun dengan algoritma kunci publik. Apabila menggunakan algoritma simetris maka

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

Protokol dasar dari *digital signature* adalah:

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

5. *Tanda tangan Digital dengan Menggunakan Public-key Algorithm dan One-way Hash Function*

Penggunaan *public-key algorithm* dalam penggunaan sehari-hari terutama untuk menandatangani dokumen yang panjang adalah tidak efesien, karena membutuhkan waktu yang sangat lama[25]. Untuk mengatasi hal ini maka protokol tandatangan digital dalam penggunaan sehari-hari adalah dikombinasikan dengan penggunaan fungsi *hash*. Selain menandatangani dokumen dengan menggunakan *private-key*, pengirim juga dapat menandatangani dokumen tersebut dengan fungsi *hash*. Penggunaan fungsi *hash* ini

---

[25] Gartner Consulting, *A White paper from GartnerGroup SET Comparative Performance Analysis*, (San Jose, 1998), p.11

akan mengefesienkan kerja komputer dalam menandatangani dokumen[26]. Langkah-langkah yang ada dalam protokol ini adalah:

1. Pengirim membuat *hash* dari suatu dokumen
2. Pengirim kemudian meng-*encrypt hash* tersebut dengan menggunakan kunci privatnya sehingga ia menandatangani dokumen tersebut.
3. Pengirim mengirim dokumen tersebut dan juga *hash* yang telah ditandatangani ke penerima.
4. Penerima kemudian membuat *hash* dari dokumen yang ia terima. Ia dengan menggunakan *key* men-*decrypt hash* yang sudah ditandatangani dengan menggunakan *public-key* dari pengirim.
5. Penerima kemudian membandingkan antara *hash* yang ia buat dan *hash* yang didapat dari pengirim. Jika hasilnya adalah sama maka tandatangan tersebut adalah valid atau sah.

6. Tandatangan Ganda (Dual Signature)

Penggunaan tandatangan ganda atau *dual signature* dalam SET adalah sangat penting, karena akan digunakan dalam berbagai bentuk transaksi pembayaran. Pada prisipnya suatu dokumen dapat ditandatangani secara berganda (*multiple signature*). Skim (*scheme*) ini akan banyak berguna dalam suatu perintah pembayaran. Contoh dari penggunaan tandatangan ganda adalah sebagai berikut: sebuah Bank mendapat perintah untuk membayarkan sejumlah uang kepada rekening/orang tertentu hanya jika ia memenuhi suatu persyaratan tertentu atau setelah terjadinya perjanjian jual-beli. Dalam transaksi ini akan terdapat dua tandatangan yaitu tandatangan dalam perintah pembayaran dan tandatangan didalam syarat pembayaran.

[26] Gartner Consulting, *Ibid*., hal 11

7. Otoritas Sertifikat (Certification Authority)

Keunggulan dari *public-key cryptography* dibandingkan dengan algoritma yang lain ternyata masih menyimpan kelemahan dalam hal keamanan (*security*), kelemahan ini adalah adanya kemungkinan pihak ke-3 yang tidak berhak menukar kunci publik milik seseorang dengan kunci miliknya. Juga terdapat ketidakpastian tentang identitas dari pemilik kunci publik. Kelemahan ini akan mengurangi keamanan dari sistem *public-key crypthography* karena seseorang dapat dengan mudah mengatakan bahwa suatu dokumen yang telah ditandatanganinya adalah tidak sah karena kuncinya telah diambil atau mengatakan bahwa kunci itu adalah bukan miliknya. Untuk mengatasi hal ini dibutuhkan adanya pihak ke-3 yang terpercaya (*Trusted Third Party*/TTP) yang dinamakan otoritas sertifikat (*Certification Authority*/CA/OS[27]) yang akan menghubungkan kunci dengan pemiliknya. Ia akan menerbitkan suatu sertifikat yang berisi identitas dari seseorang dan juga kunci privat dari orang tersebut.

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

1. Membuat kunci publik/privat miliknya sendiri.
2. Melakukan verifikasi terhadap identitas seorang calon pelanggan yang hendak meminta sertifikat dari *certification authority* tersebut. Verifikasi ini adalah berdasarkan patokan atau standar yang sudah ditentukan sebelumnya.
3. Pelanggan kemudian menyerahkan kunci publiknya kepada *certification authority*.
4. *Certification authority* kemudian mencek apakah kunci tersebut adalah pasangan dari kunci privat yang dipunyai calon pelanggan tersebut.
5. Apabila semua persyaratan tersebut sudah dipenuhi maka *certification authority* akan menerbitkan sebuah sertifikat digital (*digital certificate*) atas nama orang

---

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

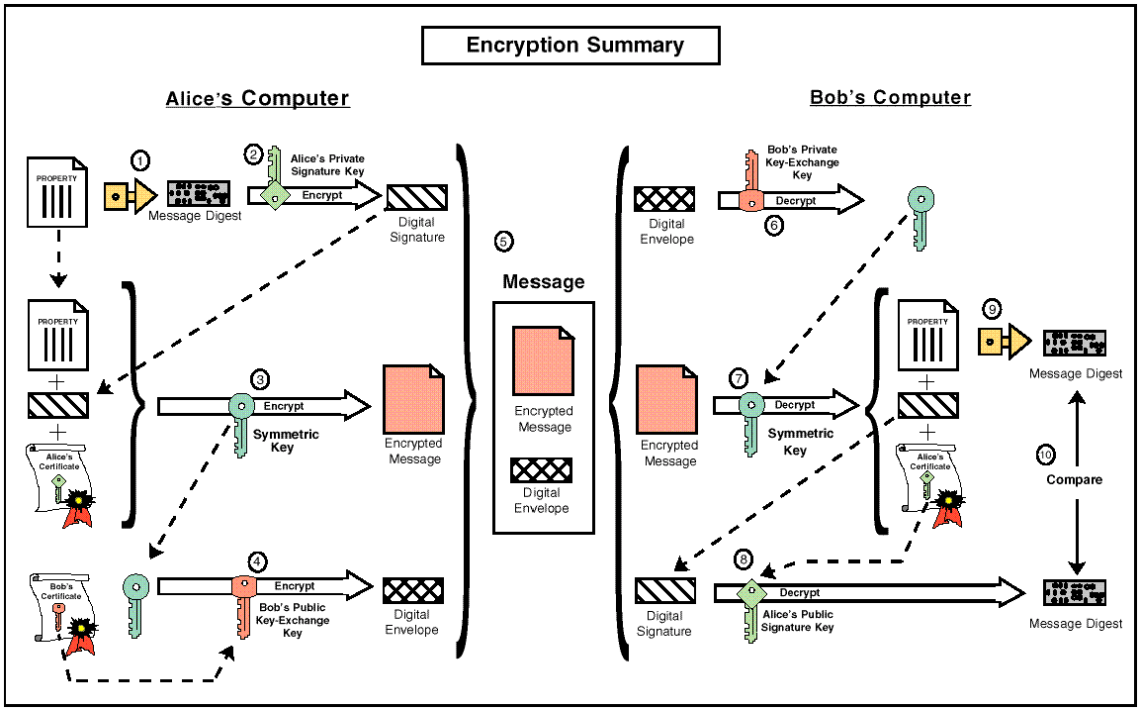
tersebut. *Digital certificate* tersebut berisi kunci duplikat dari kunci publik pelanggan dan juga identitas dari pelanggan. *Certification Authority* kemudian akan menadatangani *digital certificate* tersebut dengan menggunakan kunci privat miliknya.

8. *Penerapan Penggunaan Kriptografi dalam Penggunaanya dalam suatu Dokumen*

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

Untuk memudahkan penjelasan maka akan digunakan dua buah nama (sembarang nama) hanya untuk memudahkan ilustrasi, yaitu;

1. Alice
2. Bob



GAMBAR 2.6. RANGKUMAN DARI PENGGUNAAN KRIPTOGRAFI

Gambar diatas menunjukan proses kriptografi yang terjadi dalam *digital signature*. Langkah-langkah dalam melakukan enkripsi ini adalah sebagai berikut:

No/langkah	**Penjelasan**
1	Alice menjalankan (*runs*) data yang hendak ia kirim melalui algoritma satu arah (*one way algorithm*) sehingga ia mendapat suatu nilai (*value*) yang unik dari data tersebut. Nilai ini disebut *message digest*. Nilai merupakan semacam sidik jari bagi data tersebut dan akan digunakan dalam proses yang lebih lanjut untuk meneliti keutuhan (*integrity*) dari data tersebut.
2	Alice kemudian melakukan *encryption* terhadap *messages digest* tersebut dengan menggunakan kunci privatnya sehingga ia akan mendapatkan *digital signature* dari data tersebut.
3	Kemudian, Alice membuat (*generates*) suatu kunci simetris secara acak (*random*) dan menggunakan kunci itu untuk melakukan *encryption* terhadap data yang hendak ia kirim, tandatangan (*signature*) miliknya, dan salinan dari sertifikat digitalnya yang berisi kunci publiknya. Untuk *men-decrypt* data tersebut, Bob membutuhkan salinan dari kunci simetris tersebut.
4	Alice harus memiliki terlebih dahulu sertifikat milik Bob. Sertifikat ini berisi salinan (*copy*) dari kunci publik milik Bob. Untuk menjamin keamanan transmisi dari kunci simetris maka kunci tersebut dienkripsi dengan menggunakan kunci publik milik Bob. Kunci yang telah dienkripsi itu dikenal dengan nama amplop digital (*digital envelope*) akan dikirimkan bersama-sama dengan data yang telah dienkripsi.
5	Alice kemudian akan mengirim data (*message*) tersebut yang berisi data

	yang telah dienkripsi dengan kunci simetris, tandatangan dan sertifikat digital, serta kunci simetris yang telah di-*encrypt* dengan kunci asimetris (*digital envelope*).
6	Bob menerima pesan(*messages*) dari Alice tersebut dan kemudian *men-decrypt* amplop digital (*digital envelope*)dengan kunci privat yang dipunyainya, sehingga ia kemudian akan mendapatkan kunci asimetris.
7	Bob kemudian menggunakan kunci simetris tersebut untuk *men-decrypt* data itu (*property descryption*), tandatangan Alice, dan sertifikat miliknya.
8	Ia kemudian *men-decrypt digital signature* milik Alice dengan menggunakan kunci publik milik Alice, yang didapat Bob dari sertifikat milik Alice. Dari *decryption* ini akan didapatkan *message digest* dari data tersebut.
9	Bob kemudian memproses (*run*) data itu dengan menggunakan algoritma satu arah yang sama yang digunakan Alice untuk *message digest*.
10	Akhirnya Bob akan membandingkan antara *message digest* yang didapatkannya dari proses *decryption* diatas dengan *message digest* yang didapatkan dari *digital signature* milik Alice. Apabila hasil yang diperoleh dari perbandingan itu adalah sama, maka Bob dapat merasa yakin bahwa data tersebut tidak pernah dirusak (*altered*) selama proses transmisi dan data itu ditandatangani dengan menggunakan kunci privat milik Alice. Kalau hasil dari perbandingan itu tidak sama, maka data tersebut pasti telah diubah atau dipalsukan setelah ditandatangani.

TABEL 2.1. RANGKUMAN PENGGUNAAN KRIPTOGRAFI

E. SISTEM PEMBAYARAN DI INTERNET

Internet mengalami perkembangan yang sangat cepat baik dilihat dari segi jumlah pengguna maupun nilai bisnis didalamnya. Kalangan bisnis berusaha untuk memanfaatkan fenomena ini sebagai strategi *marketing* yang baru dan juga media penjualan yang baru. Berbagai barang dan jasa tersedia disini mulai dari barang (informasi digital) seperti *software* dan lagu sampai dengan jasa seperti layanan perbankan. Berbagai jenis barang dan jasa ini membutuhkan adanya teknologi pembayaran yang bisa melakukan transfer pembayaran secara digital terhadap barang atau jasa yang dibeli.

Terdapat banyak sistem pembayaran di internet pada saat ini. Namun pada skripsi ini pembahasan secara mendalam hanya dilakukan terhadap sistem pembayaran yang berbasis SET (*Secure Electronic Transaction*). Beberapa sistem pembayaran yang lain hanya akan dibahas secara singkat sebagai perbandingan.

Sistem pembayaran yang ada pada saat ini dapat kita kategorikan menjadi sebagai berikut :

1. Sistem debit.

   Sistem ini mengharuskan konsumen terlebih dahulu mempunyai rekening di suatu bank. Apabila ia akan melakukan suatu pembayaran maka pembayaran itu akan diambil dari rekening tersebut dengan cara di debit. Contoh dari sistem ini adalah; *Bank Internet Payment System* (BIPS), *FSTC Electronic Check* (Echeck)[28], *Open Financial Exchange* (OFX)[29].

2. Sistem kredit

   Sistem ini mengalihkan kewajiban pembayaran kepada pihak ke-3 (kredit) baru kemudian kredit ini akan ditagih kepada orang yang bersangkutan. Pedagang

---

[28] <www.echeck.org >

[29] < www.ofx.org>

akan melakukan proses *capture* yaitu meminta pembayaran dari pihak ke-3 yang menjadi perantara. Sistem ini terdiri dari *Credit Card over HTTP*/SSL dan SET. Sistem yang menggunakan SSL banyak dipergunakan oleh *internet merchant* pada saat ini. *Internet merchant* akan menggunakan SSL dalam meng-*encrypt* proses *capture* dari nomer kartu kredit yang digunakan. Sedangkan SET adalah sistem pembayaran yang akan dibahas lebih lanjut dalam skripsi ini.

3. "Tunai" atau *electronic "cash*"/*digital cash*/*e-money*

   Sistem ini merupakan salah satu perkembangan yang paling akhir dalam *internet payment*. Sistem ini dalam penggunanya mirip dengan pemakaian uang tunai dalam kegiatan sehari-hari. Kemiripan ini adalah dalam hal konsumen akan membayar koin atau uang kertas kepada penjual dalam proses pembayaran sehari-hari. Dalam sistem ini uang tunai ini akan digantikan oleh *digital token* atau suatu nilai digital (*digital value*) kepada penjual. Beberapa sistem bahkan memungkinkan penjual untuk langsung membelanjakan "uang" yang didapatnya untuk membayar suatu barang atau jasa. Sedangkan sistem yang lain mengharuskan "uang" tersebut untuk disetorkan terlebih dahulu ke dalam suatu rekening baru setelah itu bank akan menerbitkan *token* yang baru yang dapat dipakai untuk berbelanja. Beberapa contoh dari sistem ini adalah Mondex[30], Proton[31], VisaCash[32], Ecash[33], Millicent[34], CyberCoin[35], WorldPay.

---

[30] <http://www.mondex.com

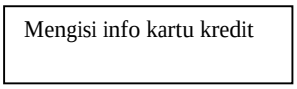
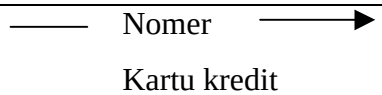
[31] <http://www.proton.be

[32] <http://www.visa.com

[33] <http://www.digicash.com

[34] <http://www.millicent.digital.com>

Berikut ini akan dijelaskan dua macam sistem pembayaran di internet dan juga akan dilengkapi alur transaksi dan diagram alur data. Tabel berikut ini menjelaskan mengenai elemen-elemen diagram alur data:

Elemen diagram	Penjelasan
Pembeli	Kepala dari setiap kolom pada diagram alur data menunjukan pihak yang melakukan transaksi
	Kotak menunjukan proses yang dilakukan oleh pihak tertentu dalam kolom itu
	Panah beserta teks menunjukan dari dan ke mana suatu data dikirimkan

Tabel 2.2 Penjelasan elemen diagram alur data

1. Toko Elektronis Sederhana dengan Forms *HTML*

"Toko" ini adalah cukup sederhana, sehingga setiap dapat dengan mudah membuka orang dapat dengan mudah membuat sebuah toko elektronik sederhana di internet. Adapun alur transaksi yang dilakukan adalah:

1. Pembeli dengan menggunakan *browser*[36] memilih barang yang akan dibelinya di *homepage* pedagang.

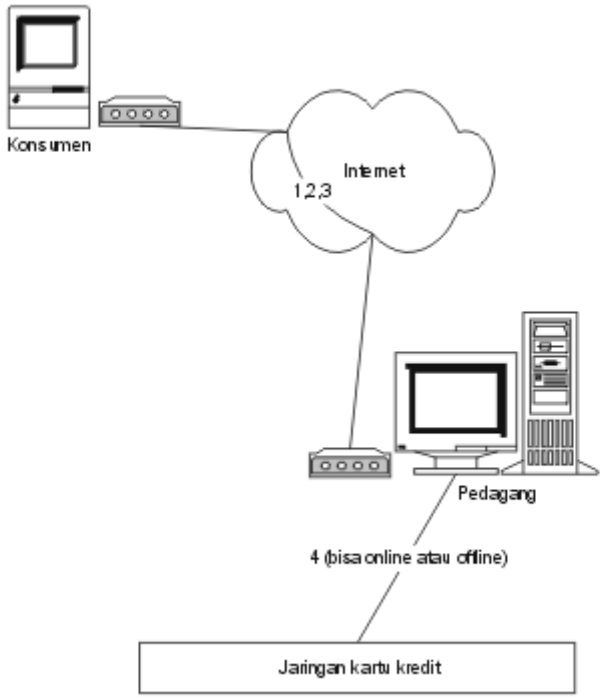
---

[35] <http://www.cybercash.com>

[36] *Browser* adalah perangkat lunak yang digunakan untuk mengakses data dari *World Wide Web*, contoh dari *browser* adalah Netscape Navigator dan Mosaic.

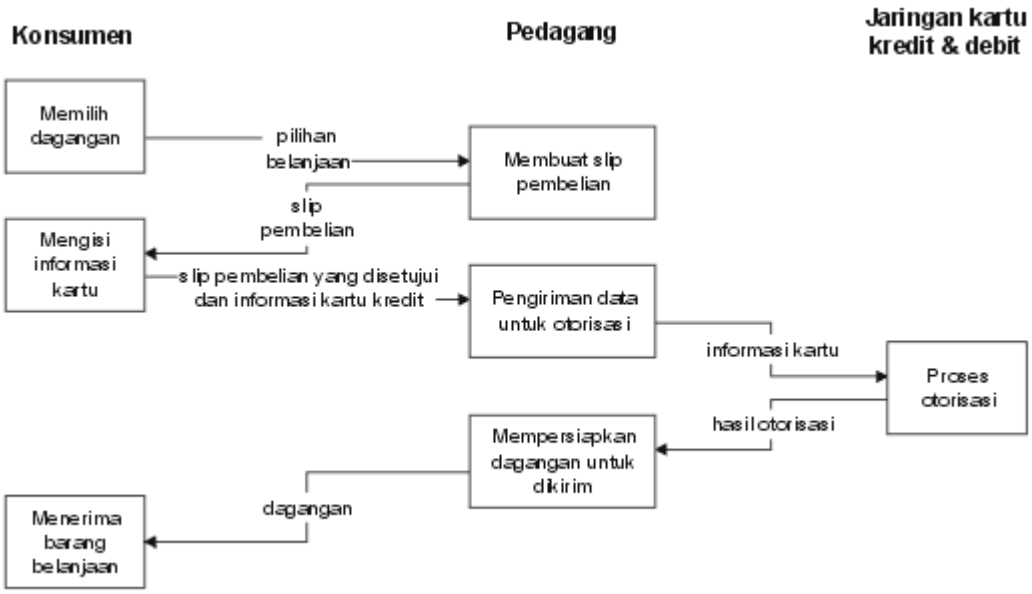
2. Setelah harga ditotal, kemudian pembeli mengisi informasi mengenai kartu kreditnya pada *form* slip pembelian yang disediakan dalam toko elektronis tersebut.
3. Informasi kartu kredit itu kemudian dikirim ke *web server* pedagang beserta informasi pembelian lainnya.
4. Informasi kartu kredit beserta informasi pembelian selanjutnya diproses sama seperti proses transaksi kartu kredit *Mail Order/Telephone Order* (MOTO).

   Jika transaksi pembayaran ini disetujui maka pedagang akan mengirim pesanan pihak pembeli.



GAMBAR 2.7 DIAGRAM TOPOLOGI TRANSAKSI
TOKO ELEKTRONIK SEDERHANA

Skenario sistem pembayaran sperti ini, tidak ada perbedaannya dengan *Mail Order/Telephone Order*, yang disebut juga dengan *card not present transaction*. Hal ini diperkenankan oleh sebagian besar lembaga pengelola kartu kredit. Konsumen akan ditagih secara biasa, sedangkan pedagang tentu akan menagih ke *acquirer* seperti halnya transaksi *MOTO*.



Gambar 2.8. Diagram alur data transaksi elektronis

Sistem sederhana ini umumnya hanya menerima kartu kredit, karena otorisasi nomer kartu kredit tidak perlu dilakukan secara *on-line*.

Pada dasarnya tidak ada fasilitas keamanan pada sistem pembayaran ini. Jika pedagang tidak menggunakan *web server* yang aman, maka seluruh kelemahan pada protokol HTTP dan TCP/IP akan dimiliki oleh sistem ini. Orang lain akan dengan mudah mendapat informasi kartu kredit. Pada beberapa situs sudah menggunakan *web server* dari Netscape yang mendukung SSL. Dengan cara ini terdapat "saluran" komunikasi yang aman antara pembeli dan pedagang. Pedagang pada akhirnya tetap dapat membaca informasi kartu kredit milik pembeli. Seorang pedagang yang berniat tidak baik dapat menggunakan informasi kartu itu secara berulang-ulang. Selain itu, jika

pedagang tidak melakukan otorisasi sebelum mengirimkan barang dagangannya kepada pembeli, maka pedagang akan menanggung resiko tertipu oleh pembeli.

2. Secure Electronic Transaction (SET)

a. Deskripsi

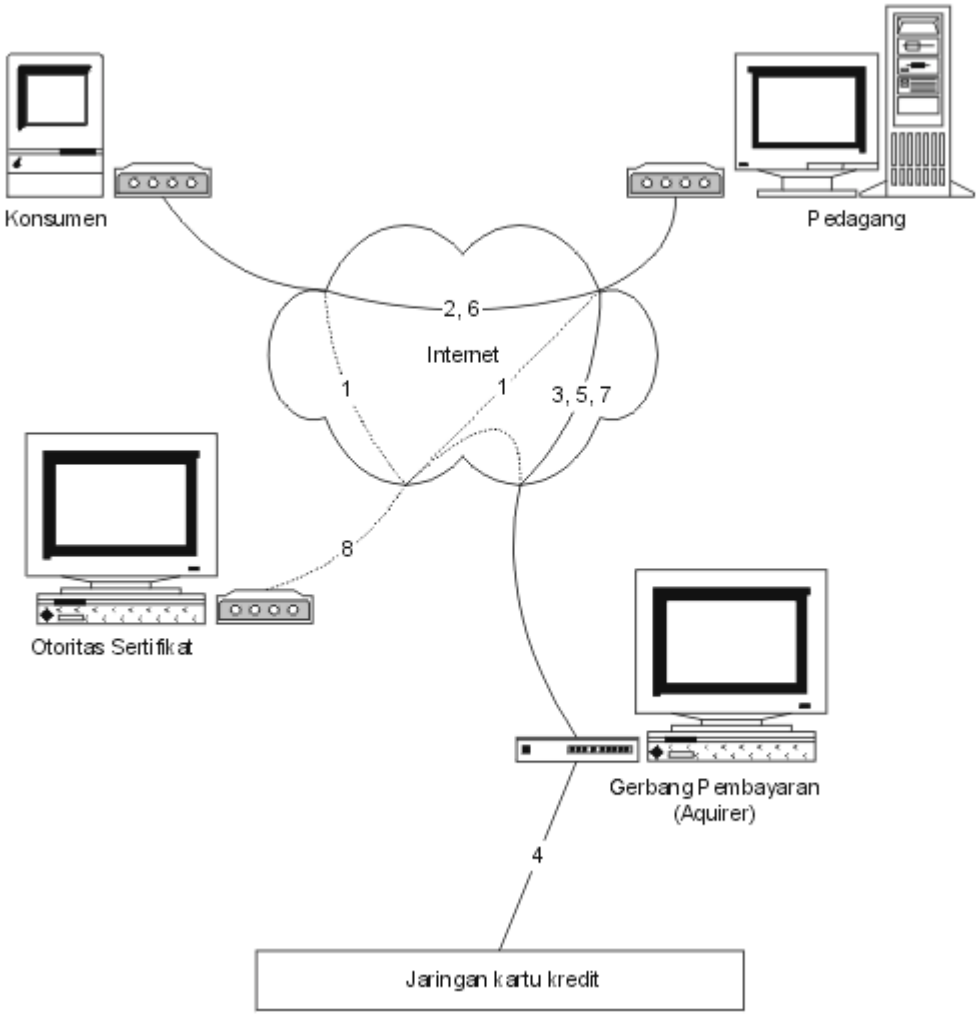
Toko elektronis tersebut diatas mempunyai beberapa keunggulan dan juga kelemahan. Keunggulannya adalah kemudahan pembuatan dan juga biaya yang relatif murah dalam membuatnya. Selain itu sistem ini memiliki kelemahan yaitu meskipun segala informasi kartu kredit dapat dikomunikasikan (dipertukarkan) dengan aman tetapi tidak terdapat cara untuk menentukan identitas dari pedagang (penerima). Tidak adanya cara untuk menentukan identitas dari pedagang mengakibatkan pembeli tidak dapat mengetahui apakah ia adalah seorang pedagang yang sah (*legitimate*) ataukah ia adalah seorang penjahat yang sedang mengumpulkan informasi kartu kredit (nama, nomor kartu). Resiko ini dapat mengakibatkan kerugian baik bagi konsumen, pedagang maupun perusahan kartu kredit.

Problem tersebut diatas kemudian melahirkan suatu sistem pembayaran yang baru yang digagas oleh MasterCard dan Visa. Skim ini juga didukung oleh berbagai penyedia layanan transaksi yang aman (*secure transaction company*) seperti GTE, IBM, Microsoft, Netscape, Saic, Terisa systems, Verisign. GTE dan IBM menyediakan *switches* dan *banking network* bagi protokol ini, Microsoft dan Netscape menyediakan *browser* dan dan *server transaction software*. Verisign dan GTE akan menyediakan mekanisme untuk melakukan otentifikasi terhadap sertifikat yang akan digunakan oleh pembeli, penjual dan juga perusahaan kartu kredit. SET mengakomodasikan kebutuhan kalangan bisnis dalam hal transaksi pembayaran dengan kartu kredit yang aman, yaitu:

1. Menyediakan keamanan dan kerahasiaan bagi informasi pembayaran dan pemesanan. Adalah hal yang sangat penting untuk menjamin pemegang kartu

kredit bahwa informasi ini adalah aman dan hanya dapat dibaca oleh orang yang dikehendakinya. Keamanan dan kerahasiaan juga akan mengurangi resiko kejahatan yang dilakukan oleh pihak ketiga yang akan mengambil ditengah jalan (*intercept*) informasi tersebut.

2. Jaminan bagi keutuhan (*integrity*) terhadap seluruh data yang ditransmisikan. Jaminan keutuhan ini akan menjamin bahwa tidak akan ada perubahan terhadap isi pesan yang dikirimkan. SET menggunakan *digital signature* untuk menjamin bahwa isi yang terdapat dalam setiap pembayaran dan pemesanan akan diterima sama dengan sewaktu pesan itu dikirim.
3. Terdapat mekanisme otentifikasi terhadap pemegang kartu kredit sebagai pemilik rekening. SET menggunakan mekanisme *digital signature* dan otorisasi terhadap pemegang kartu untuk verifikasi apakah ia adalah seorang yang berhak dan rekening itu benar miliknya.
4. Terdapat mekanisme otentifikasi bahwa seorang penjual dapat meng-*accept* karena ia memiliki hubungan dengan lembaga keuangan (*acquire*r).



GAMBAR 2.8 DIAGRAM TOPOLOGI PROTOKOL SET

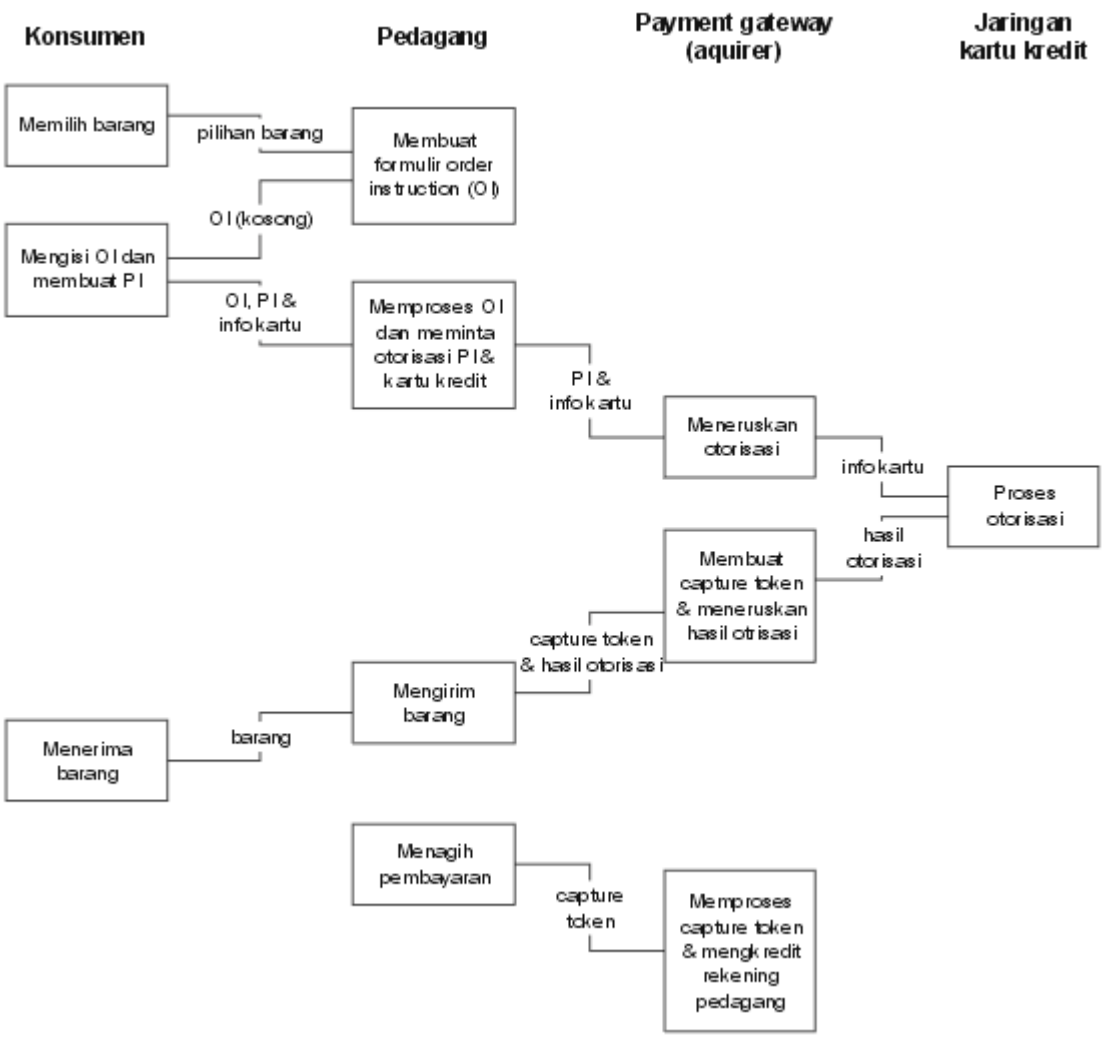


Diagram Alur Data SET

b. *<u>Perangkat</u>* *<u>lunak</u>*

Secure Electronic transaction (SET) tidak hanya dirancang untuk transaksi di *web* saja , namun juga bisa digunakan pada media yang lain. Pedagang dapat menyebarkan katalog dalam CD-ROM. Pembeli dapat memilih barang yang akan dibelinya di katalog tersebut, dan kemudian dapat membelinya dengan cara mengontak pedagang tersebut

baik dengan menggunakan *browser* maupun dengan menggunakan surat elektronis (*e-mail*).

c. *Alur transaksi*

Secara singkat, alur transaksi pada protokol SET dapat dijelaskan sebagai berikut;

1. Untuk melakukan transaksi SET, pembeli dan pedagang harus terlebih dahulu mendapatkan sertifikat dari otoritas sertifikat/*Certification Authority* (OS). Pembeli dalam langkah ini harus mengetikkan *personal account number* (PAN) dan informasi jati dirinya. Pedagang dalam langkah ini harus juga memberikan informasi jati dirinya kepada OS.
2. Pembeli kemudian dapat mulai bebelanja. Jika sudah memilih barang yang hendak dibeli, pembeli membuat *order instruction* (OI) dan *payment instruction* (PI). Pembeli kemudian menyerahkan OI dan PI kepada pedagang. PI tidak dapat dibaca oleh pedagang karena di-*encrypt* dengan menggunakan kunci publik milik gerbang pembayaran (*payment gateway*).
3. Setelah pedagang memproses OI, maka pedagang melakukan otorisasi PI melalui gerbang pembayaran. Seringkali *acquirer* bertindak sebagai gerbang pembayaran.
4. Gerbang pembayaran melakukan otorisasi kartu kredit dengan *issuer* melalui jaringan privat kartu kredit.
5. Jika otorisasi disetujui, maka gerbang pembayaran menginstruksikan pedagang untuk menyerahkan barang dagangan kepada pembeli.
6. Pembeli menerima barang yang dibelinya.
7. Pedagang kemudian dapat memperoleh pembayaranya dengan melakukan proses *capture* melalui gerbang pembayaran pula. Langkah ini sering di-*batch*, sehingga akan ada tenggang waktu antara permintaan pembayaran (*payment capture*) dengan proses otorisasi.

8. Setiap melakukan komunikasi, para pihak yang terlibat dalam transaksi dapat melakukan otentifikasi terhadap sertifikat digital (*digital certificate*) milik pihak yang lain dengan mengakses situs *Certification Authority* nya.

Berdasarkan skenario diatas, terlihat bahwa sistem perdagangan di internet dengan skenario SET dijalankan secara *on-line*. Protokol SET dapat mendukung sistem pembayaran dengan *charge card* maupun dengan kartu kredit.

Pembeli dapat dilihat jati dirinya oleh pedagang, begitu juga sebaliknya. Baik pembeli maupun pedagang dapat saling memeriksa sertifikat digital yang dipertukarkan. Meskipun demikian, pedagang tidak dapat mengetahui informasi kartu kredit pembeli.

d. *Keamanan dan Serangan*

Inti dari keamanan dalam protokol SET adalah penggunaan *digital certificate* dan *digital signature*. Secara teoritis, tanpa serangan dengan mencoba semua kemungkinan kunci (*brute-force attack*), sertifikat digital dapat bertahan dari penipuan dari pihak ketiga yang bertindak sebagai pihak yang asli (*men in the middle attack*) dan juga serangan dengan mengulang pesan (*replay attack*). Hal ini disebabkan karena siapapun yang ingin melakukan pemeriksaan dapat memastikan apakah kunci publik yang diterimanya sah atau tidak. Seperti sudah diterangkan sebelumnya, bagian yang rentan dari kemungkinan penyalahgunaan sertifikat adalah saat pemberian sertifikat digital otoritas sertifikat utama kepada pihak-pihak yang lain yang memerlukan seertifikat digital, seperti kepada para pengembang perangkat lunak untuk SET.

Dalam sertifikat pembeli tidak terdapat informasi kartu pembeli, yaitu *personal account number* (PAN) dan tanggal kadaluarsanya, namun berisi hash dari PAN, tanggal kadaluarsa dan juga sederatan angka rahasia yang hanya diketahui oleh pembeli (*personal identification number*/PIN). Jadi jika pedagang memeriksa sertifikat milik seorang pembeli, maka meskipun melihat jati diri pembeli, pedagang tetap tidak dapat melihat informasi kartunya.

Seorang penyerang yang memiliki sertifikat seorang pembeli juga tidak dapat menggunakanya tanpa mengetahui informasi kartu dan juga PINnya. Informasi kartu dan PIN dalam skenario SET dikirimkan dalam bentuk terenkripsi kepada gerbang pembayaran untuk pemeriksaan. Gerbang pembayaran tidak hanya memeriksa keabsahan sertifikat digital milik pembeli, tetapi juga memeriksa apakah *hash* dari informasi kartu dan angka rahasia sesuai dengan nilai hash yang ada dalam sertifikat.

Ukuran kunci yang dipergunakan dalam SET sangat panjang dan dapat dikategorikan sebagai kunci yang sulit dijebol (*hard encryption*). Semua kunci berukuran 1024 bit, kecuali untuk kunci OS utama yang menggunakan ukuran kunci 2048 bit. Kunci sepanjang ini sulit dipecahkan dengan serangan yang mencoba semua kemungkinan kunci (*brute-force attack*).

Protokol SET juga menggunakan suatu perangkat kriptografi baru, yaitu tandatangan pesan ganda (*dual signature*). Dengan menggunakan tandatangan pesan ganda tersebut, gerbang pembayaran saat melakukan otorisasi dapat memastikan bahwa PI yang diterimanya memang benar berhubungan dengan suatu OI tertentu, namun gerbang pembayaran tetap tidak tahu isi OI tersebut.

e. *Kepercayaan dan penipuan*

Karena mengandalkan sertifikat digital, maka tentunya pihak-pihak yang bertransaksi mengandalkan kepercayaan mereka terhadap OS yang menerbitkan sertifikat digital. Sama halnya dengan transaksi menggunakan kartu kredit, tentunya pembeli harus mempercayai lembaga keuangan pengelola kartu kredit yang melakukan otorisasi.

Untuk pemeriksaan serifikat digital, maka tentunya pihak-pihak yang bertransaksi juga membutuhkan informasi dari OS mengenai sertifikat siapa saja yang dibatalkan (*revoked*). Tentunya OS yang menyimpan daftar sertifikat dibatalkan ini harus dapat dipercayai oleh pihak-pihak yang melakukan transaksi.

Skenario protokol SET tidak memuat spesifikasi pencatatan yang dilengkapi dengan tandatangan digital dari pihak-pihak yang melakukan transaksi. Namun dalam implementasinya, pencatatan dapat dilakukan diperangkat lunak klien yang dipergunakan oleh pembeli dan juga di *web server* pedagang.

f. *Penerimaan Pembayaran dan Biaya Transaksi*

Spesifikasi SET tidak menjelaskan mengenai biaya tambahan atas transaksi. Namun, jika pihak *acquirer* sendiri yang menjadi gerbang pembayaran, tentunya boleh dikatakan tidak ada biaya tambahan. Jadi hampir tidak ada bedanya dengan transaksi kartu kredit biasa, karena dalam transaksi kartu kredit on-line yang biasa, pedagang akan melakukan otorisasi itu melalui *acquirer* juga.

Seperti sudah dijelaskan diatas, karena perubahan sistem dimana pedagang tidak mendapatkan informasi kartu kredit, maka memang ada perubahan prosedur penagihan ke *acquirer*.

g. *Kontrak Pembayaran dengan Menggunakan Digital Signature*

SET menggunakan sistem keamanan yang berjenjang (hirarkis) untuk memvalidasi hubungan antara lembaga keuangan dan para pihak yang terlibat. Sistem keamanan ini merupakan kombinasi dari *Public Key Encryption*, *digital signature, digital certificate* dan juga *Certification Authority*. Pemilik kartu kredit yang hendak melakukan transaksi pembayaran dengan menggunakan SET, pertamakali harus mempunyai kartu kredit dari lembaga keuangan yang mendukung SET. Setelah itu ia juga harus mempunyai *digital/virtual wallet*[37]. "Dompet" ini akan berisi nama

[37] *Virtual Wallet* adalah suatu *software* yang akan diinstalasikan ke dalam komputer pengguna. Duna dari software ini adalah untuk menyimpan kartu kredit virtual yang diberikan oleh bank.

pelanggan, nomor kartu kredit dan jangka waktu berlakunya kartu tersebut. Dompet ini juga akan dipergunakan untuk menyimpan *digital receipt* yang didapat pengguna tersebut dalam setiap pembelian yang ia lakukan. Namun kegunaan utama dari "dompet" ini adalah juga digunakan untuk melakukan komunikasi dengan *software* SET milik pedagang dengan men-*download digital certificate* milik pedagang dan melakukan verifikasi terhadap *digital certificate* milik pedagang tersebut. Dari Vwallet ini juga dapat diketahui hubungan antara pedagang dan lembaga keuangannya (bank).

Langkah kedua yang harus dilakukan adalah mengajukan aplikasi untuk mendapatkan sertifikat digital dari *Certification Authority*/OS. Sertifikat digital pada asasnya bisa didapatkan dari setiap *Certification Authority* yang ada di dunia termasuk dari Verisign yang berkedudukan di USA[38]. Setelah dilakukan pengecekan terhadap identitas pengguna dan juga ia teleh memenuhi semua persyaratan dalam berlangganan maka *Certification Authority* akan memberikan sertifikat digital dan juga sepasang kunci kepadanya. Sekarang ia telah siap untuk melakukan transaksi yang aman (*secure*) baik secara teknis maupun hukum didalam *e-commerce*. Seperti juga halnya dengan pemegang kartu kredit, pedagang juga harus mempunyai *software* khusus dan juga sertifikat digital sebelum ia dapat melakukan transaksi jual beli dalam skim SET. *Software* milik pedagang ini akan melakukan validasi terhadap sertifikat digital milik pemilik kartu dan juga hubungan antara pemilik kartu dengan lembaga keuangannya (bank). Maksud dari hubungan ini adalah apakah pemebeli memang memliki kartu kredit yang valid yang dikeluarkan oleh lembaga keuang teresbut.

---

[38] Secara teknis adalah dimungkinkan penggunaan sertifikat digital dari certification auhority yang berkedudukan dimana saja didunia, selama certification auhority itu mempunyai hubungan (terhubung dalam *root*). Tetapi secara legal yuridis hal ini dapat menimbulkan masalah, karena hal ini adalah menyankut kedudukan hukum, penggunaan hukum yang dipakai dari pengguna tersebut.

Seorang pengguna kartu kredit apabila akan berbelanja, maka ia pertamakali akan memilih barang-barangnya pada *web-site* pedagang. Pedagang kemudian akan mengirimkan perintah pembayaran dan sertifikat digital miliknya. Pada saat pemegang kartu kredit memilih cara pembayaran, maka sertifikat digital miliknya akan secara otomatis dikirimkan kepada pedagang. *Software* SET yang dimiliki oleh keduabelah pihak akan secara simultan melakukan verifikasi terhadap sertifikat digital dan tandatangan digital yang terdapat perintah pembayaran. Penggunaan *digital signature* dalam SET inilah yang akan menjadi pembahasan yang utama dalam skripsi ini.

BAB III

TINJAUAN HUKUM TERHADAP PERINTAH PEMBAYARAN BERBASIS SET (SECURE ELECTRONIC TRANSACTION)

A. PERJANJIAN ELEKTRONIS DALAM PERSPEKTIF YURIDIS

Payment instruction dengan menggunakan *Digital signature* dalam sistem pembayaran SET pada dasarnya adalah suatu perikatan berdasarkan hukum di Indonesia. Perintah pembayaran dengan menggunakan *digital signature* disini adalah perikatan yang bersumber dari perjanjian. Pengertian dari perjanjian adalah suatu peristiwa dimana seseorang berjanji kepada orang lain atau dimana dua orang atau lebih itu saling berjanji untuk melaksanakan suatu hal[39]. Dari peristiwa ini (perjanjian) timbul suatu hubungan hukum antara kedua orang tersebut yang dinamakan perikatan (*verbintenis*). Di dalam BW, perjanjian diatur dalam pasal 1313 yaitu, suatu perjanjian adalah suatu perbuatan dengan mana satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih.

Perjanjian (*overeenkomst*) diatur dalam buku ke-3 BW (KUHPer), buku ke-3 ini mempunyai sifat terbuka. Maksud dari sifat terbuka ini adalah para pihak bebas untuk melakukan perjanjian diantara mereka, meskipun perjanjian itu tidak diatur di dalam BW. Perjanjian yang dibuat antar para pihak ini pada dasarnya tidak harus dibuat dalam bentuk tertentu (tertulis). Perjanjian-perjanjian yang ada pada galibnya berbentuk bebas. Perjanjian itu dapat diadakan dalam bentuk lisan dan apabila diterakan dalam suatu tulisan, itu sering kali mempunyai sifat alat pembuktian semata-mata[40]. Meskipun

---

[39] Subekti, SH., *Hukum Perjanjian*, cetakan ke-12 (Jakarta: Intermasa, 1990), hal.1

demikian terdapat beberapa perjanjian disyaratkan adanya bentuk tertulis, bahkan diharuskan adanya akta notaris (hibah, pengesahan atas tanah yang terdaftar, pembentukan Perseroan terbatas).

Syarat "tertulis" dari suatu perjanjian berdasarkan pendapat diatas adalah sangat relatif dan hanya mempunyai sifat pembuktian semata. Pitlo dalam bukunya *Bewijs en Verjaring Naar het Nederlands Burgerlijk Wetboek* memberikan definisi surat yang diberikan oleh para ahli hukum pembuat BW adalah, "pembawa tanda bacaan yang berarti, yang menerjemahkan suatu isi pikiran. Atas bahan apa dicantumkannya tanda bacaaan tersebut adalah tidak penting". Perkembangan yurisprudensi di Indonesia pada saat ini juga telah menunjukan perkembangan yang baik, yaitu diterimanya *faxsimile* sebagai alat bukti dalam putusan Mahkamah Agung RI No. 9K/N/1999[41]. Bukti berupa *faxsimile* dapat diterima sebagai bukti tulisan, perkembangan ini tentu sangat bagus dalam mendukung kegiatan bisnis pada saat ini. Berdasarkan pendapat tersebut diatas sebenarnya adalah tidak merupakan suatu masalah apabila suatu perjanjian itu dibuat/dituangkan dalam bentuk atom-atom tinta diatas kertas ("tertulis" dalam anggapan konvensional) ataupun dalam bentuk bit-bit data ("tertulis" dalam era komputer/dalam penggunaan *digital signature*).

Meskipun seringkali tulisan itu hanya dibutuhkan untuk masalah pembuktian, terdapat syarat bahwa untuk perjanjian tertentu (hibah/pembentukan PT) haruslah dibuat dalam bentuk akta dibawah tangan atapun akta notaris. Apabila kita mengartikan syarat tertulis tersebut secara harfiah maka perjanjian dalam bentuk *digital signature* adalah sukar untuk dapat dimasukan dalam kategori ini. Persyaratan adanya akta dalam bentuk tertentu ini sifatnya adalah memaksa dan apabila tidak diidahkan, perbuatannya lantas

---

[40] H.F.A. Vollmar, *Pengantar Studi Hukum Perdata*, jilid 2 (Jakarta, RajaGrafindo persada:1995), hal. 128. Elips, *Pengembangan Hukum Ekonomi*, (Jakarta:Elips, 1998), hal.21

[41] Widjanarto, "Dampak Implementasi Undang-undang Kepailitan Terhadap Sektor Perbankan" *Jurnal Hukum Bisnis* (volume 8, 1999) :79

batal[42]. Sedangkan dalam perbuatan hukum lainnya secara umum bentuk tulisan hanya mempunyai arti sebagai alat bukti, yang hanya memperoleh arti sebagai alat bukti yang hanya memperoleh arti apabila perjanjiannya dibantah.

File komputer (*text*, *bitmap*, *sound*) yang di-*encrypt* dengan menggunakan *digital signature* seperti disebutkan diatas dapat dipakai sebagai media dalam membentuk suatu perjanjian. *File* komputer dari *digital signature* dapat digunakan sebagai bahan pembuktian, karena pada umumnya bahan pembuktian adalah bebas. Para pihak juga berwenang untuk mengadakan perjanjian apa saja yang akan berlaku sebagai bukti antara mereka (perjanjian bukti/perjanjian penetapan/*bewijsovreenkomst*) seperti yang ada dalam *Arres* HR 3 Mei 18 [43]. Maksud dari perjanjian penetapan adalah perjanjian-perjanjian yang disitu ditetapkan, apakah yang akan merupakan hal yang menurut hukum bagi para pihak tanpa bahwa disitu ada maksud untuk menciptakan hak-hak dan/atau kewajiban-kewajiban baru[44]. Perjanjian ini tidak bersifat *obligator* dan *dispositif* tetapi *deklaratif* (menerangkan, menyatakan). Hal itu tidak menimbulkan sesuatu yang baru, tetapi mempertetapkan apa-apa yang menurut penglihatan dari para pihak haruslah dipandang sebagai suatu perhubungan hukum yang ada. Perjanjian-perjanjian seperti ini adalah dimungkinkan dan sah berdasarkan aturan umum hukum perjanjian (*arres* HR 25 Juni 1926, 2 Desember 1927,9 Januari 1941).

Tandatangan dalam Perspektif Yuridis

---

[42] Vollmar, op. cit., hal.129

[43] *Ibid.,* hal. 475

[44] *Ibid.,* hal 135

Orang pada umumnya berpendapat bahwa suatu akta sudah sepatutnya ditandatangani. Tandatangan ini menyebabkan orang yang menandatanganinya mengetahui isi dari akta yang ditandatanganinya. Orang tersebut juga terikat dengan pada isi dari akta tersebut[45].

Tandatangan yang dibubuhkan dalam suatu kontrak tidak harus dilakukan "secara langsung" seperti seseorang membubuhkan tandatangan. Tandatangan itu bisa juga dalam bentuk stempel atau bentuk lainnya. Syarat dari digunakannya tandatangan selain tandatangan "konvensional" adalah harus digunakan secara teratur. Keterangan/kontrak yang sudah dibubuhi "tandatangan" tersebut lantas dianggap memang berasal dari orang yang tandatangannya tertera diatasnya dan orang tersebut lantas terikat oleh keterangan tersebut[46].

Tandatangan bukan merupakan bagian yang penting (substansi) dari suatu transaksi/kontrak, tapi kehadirannya dilihat atau diperhatikan karena keberadaannya atau bentuknya (*form*)[47].

Penandatanganan suatu dokumen secara umum mempunyai tujuan sebagai berikut:

1. Bukti (*evidence*): suatu tandatangan akan mengotentifikasikan penandatangan dengan dokumen yang ditandatanganinya. Pada saat penandatangan

---

[45] *Ibid.,* Vollmar, hal. 478

[46] *Ibid.,* Vollmar, hal. 142

[47], Information Security Committee, Electronic Commerce and IT Division,American Bar Association, *Digital signature Guidelines*, (Chicago: ABA,1996)

membubuhkan tandatangan dalam suatu bentuk yang khusus, tulisan tersebut akan mempunyai hubungan (*attribute*) dengan penadatangan[48].

2. *Ceremony*: Penandatanganan suatu dokumen akan berakibat penandatangan akan tahu bahwa ia telah melakukan suatu perbuatan hukum, sehingga akan mengeliminasi kemungkinan adanya *inconsiderate engagement*[49].
3. Persetujuan (*approval*): dalam penggunaanya dalam berbagai konteks baik oleh hukum atau oleh kebiasaan, tandatangan melambangkan adanya persetujuan atau otorisasi terhadap suatu tulisan, atau penandatangan telah secara sadar mengetahui bahwa tandatangan tersebut mempunyai konsekwensi hukum[50].
4. *Efficiency and Logistics*: tandatangan dalam suatu dokumen tertulis seringkali menimbulkan kejelasan dan keabsahan dari suatu transaksi dan juga akan mengurangi kebutuhan untuk mengecek keabsahan suatu dokumen kepada orang yang bersangkutan[51].

---

[48] Lon L.Fuller, *Consideration and Forms*, 799, 800 (1941); Jeremy Bentham, *The works of Jeremy Bentham*, 508-585 (Bowring Ed.,1962). Bentham menyebutkan tindakan untuk membuat suatu bukti sebagai *Preappointed* (*i.e. made in advance evidence*).

[49] John Austin, *Lectures on Jurisprudence* (4th ed., 1873) hal. 939-944; Lon L. Fuller, hal. 400: Rudolf von Jhering, *Geist Des Rosmichen Rechts* (8th ed.,1883) hal. 494-498

[50] Model Law on E-Commerce, Uncitral 29th sess., pasal 7 (1), UN Doc. A/CN.9/XXXIX/CRP.i/Add.13 (1996)

[51] *loc. cit.*, Fuller, hal 801-882; *loc..cit*., Jhering, hal. 494-497

B. TINJAUAN YURIDIS PENGGUNAAN DIGITAL SIGNATURE DALAM SET

SET menggunakan kombinasi antara *message digest* yang berasal dari fungsi *hash* (*hash function*) dan *encryption* yang menggunakan kunci privat untuk menandatangani *data message*. Fungsi *hash* yang digunakan di dalam SET akan menghasilkan 160-bit *message digest*[52]. Dengan menggunakan algoritma ini kemungkinan untuk menemukan 2 buah *data messages* yang mempunyai *message digest* yang sama adalah 1 diantara 10 pangkat 48[53]. *Message digests* ini kemudian akan di-*encrypt* dengan menggunakan kunci (*key*) yang menggunakan algoritma RSA yang mempunyai panjang 1024 bit. Hasil dari enkripsi inilah yang kemudian disebut sebagai *digital signature*.

1. Para Pihak dalam Payment Instrustion yang berbasis SET

Perintah pembayaran (*payment instruction*) yang menggunakan SET melibatkan beberapa pihak selain dari pembeli(*cardholder*) dan penjual (*merchant*). Para pihak itu adalah *payment gateway*, *acquirer* dan *issuer*. Para pihak ini terhubung secara *on-line* melalui jaringan internet ataupun secara *off-line* (melalui jaringan privat). Keberadaan para pihak adalah bersifat "maya" atau *virtual* karena kita "tidak tahu" keberadaanya/domisilinya kita hanya tahu domisilinya berdasarkan *digital certificate* yang dimilikinya.

Proses pembayaran di dalam SET adalah berawal dari pembeli/*cardholder* (lihat gambar 2.8.) Proses ini adalah kebalikan dari proses pembayaran kartu kredit yang kita

---

[52] Visa and MasterCard, *SET Secure Electronic Transaction spesification Book1: Business Description Version 1.0,* (Visa and MasterCard, 1997), hal 17

[53] *Ibid*.,

kenal selama ini (konvensional) yang berawal dari penjual. Didalam *Payment Instruction* (PI) dan *Order Information*(OI) pembeli berkedudukan sebagai *originator* seperti yang diatur dalam pasal 2 ayat b *Uncitral Model Law on Electronic commerce* (selanjutnya disebut dengan *Model Law* saja). *Merchant* dan *Payment gateway* berkedudukan sebagai *addresse* (pasal 2 ayat d *Model Law*). PI dan *Order Instruction* (OI) yang dibuat oleh *addresse* kemudian akan dikirimkan kepada *merchant*. PI ini kemudian akan diteruskan oleh *merchant* kepada *payment gateway*. *Merchant* berkedudukan sebagai *addresse* hanya terhadap OI saja, sedangkan terhadap PI ia berkedudukan sebagai perantara. Merchant akan meneruskan PI ini ke *Payment gateway*. PI ini setelah diverifikasi oleh *merchant* akan dikirimkan ke *payment gateway* untuk diproses lebih lanjut (proses otorisasi).

Pembedaan antara *originator* dan *addressee* ini adalah sangat diperlukan dalam proses pembayaran SET. Pembedaan ini akan menentukan dan kewajiban dari para pihak. Apabila terjadi kesalahan atau gangguan (*failure*) dalam sistem maka kita akan dengan mudah mengetahui siapakah yang bertanggungjawab.

Pengolahan data dari *data messages* di SET sejak data itu pertamakali diciptakan hingga proses ini selesai dilakukan secara otomatis oleh *software* SET yang dimiliki para pihak. Keterlibatan para pihak dalam pengolahan data sangat minimal[54]. Mereka tidak (harus) mengetahui berapakali *data messages* itu berpindah (*re-directing*) dari satu *server* ke *server* yang lain. Mereka hanya perlu mengetahui bahwa benar pesan yang dikirimnya akan sampai ditempat yang ditujunya.

2. Payment Instruction dengan Menggunakan Digital signature

---

[54] *Ibid.,*

Perintah pembayaran didalam SET dimulai dengan adanya inisiatif dari pembeli (*cardholder*). Apabila pembeli hendak berbelanja dan hendak membayar maka *software* yang dimilikinya mengecek keabsahan *digital certificate* dari *merchant*, *payment gateway* ke *root*[55]. *Software* yang dimiliki oleh *cardholder* kemudian akan membuat OI dan PI dan meletakkan *transaction identifier* yang sudah ditandatangani oleh *merchant* ke dalam OI dan PI tersebut.

Software yang dimiliki oleh *cardholder* kemudian akan membuat sebuah *dual signature* untuk OI dan PI tersebut. Caranya adalah dengan membuat *message digest* dari OI dan PI, *message digest* ini kemudian akan dikirimkan bersama dengan *dual signature* (lihat gambar 2.8 mengenai jalanya transaksi ini). Akhirnya *software* akan mengirimkan message yang berisi OI dan PI ke *merchant*.

Software yang dimiliki oleh *merchant* kemudian akan menerima pesan tersebut. Proses selanjutnya adalah melakukan verifikasi terhadap *digital certificate* yang dipunyai oleh *cardholder* ke *root*. Kemudian akan dilakukan pengecekan terhadap *message digest* dari PI (dan juga OI) untuk mengecek keabsahan dari *digital signature* tersebut. Pengecekan ini dilakukan unutk mengetahui apakh pesan tersebut pernah dirusak (*tempered*) sejak pertamakali ia dibuat. Setelah prosese ini selesai maka setelah ditandatangani oleh *merchant* maka PI akan dikirimkan ke *payment gateway*. Apabila otorisasi yang dilakukan oleh *payment gateway* disetujui maka transaksi pembayaran ini sudah selesai. *Merchant* akan melakukan prestasi yang dijanjikan, pembeli akan menerima *purchase response* yang dapat disimpan didalam *virtual wallet*.

a. Pengakuan Yuridis atas Data Messages

---

[55] *Ibid*., Set book 1, hal 50

Seluruh *data messages* yang dikirimkan oleh para pihak dalam SET adalah menggunakan *digital signature*. *Data message* ini mempunyai sifat yang hampir sama dengan kontrak diatas kertas. Pesan ini senantiasa dapat diakses (dapat dilihat), dapat diperiksa orisinalitasnya (dengan mengecek *message digest*), dapat mengidentifikasikan penandatangannya (ditandatangani dengan menggunakan kunci privat penandatangan). Pesan ini juga menunjukan kecakapan bertindak dari penandatangan, yaitu dengan adanya *digital certificate* sebagai lampiran.

Berdasarkan hal tersebut diatas berdasarkan paal 5 *Uncitral Model Law on electronic commerce* (selanjutnya disebut *Model Law*) *data messages* ini mempunyai kekuatan hukum dan dapat dijalankan secara hukum (*enforceability*). Hal ini dikarenakan pesan-pesan ini mempunyai sifat-sifat yang dipunyai oleh kontrak-kontrak konvensional yang biasa kita kenal. Sehingga berdasarkan pasal ini *data messages* ini mempunyai kekuatan yuridis.

Model Law menyatakan beberapa persyaratan agar suatu pesan dapat masuk kedalam kriteria "*writing*". Kriteria-kriteria ini diambil dari norma-norma hukum yang ada didalam sistem-sistem hukum yang ada di dunia. Norma itu ada yang berasal dari ketentuan perundangan, kebiasaan dan yang berasal dari yurisprudensi. Kriteria yang dipakai adalah:

1. Adanya bukti yang cukup yang dapat membuktikan adanya kata sepakat dari para pihak;
2. Memberitahukan kepada para pihak bahwa perbuatan yang dilakukannya ini mempunyai akibat hukum;
3. Mempertahankan keberadaan dokumen tersebut (dokumentasi) untuk suatu jangka waktu tertentu;
4. Memungkinkan dilakukannya otentifikasi terhadap dokumen tersebut dengan menggunakan "tandatangan" yang ada;
5. Memudahkan verifikasi yang dilakukan oleh pemerintah atau untuk kepentingan pengadilan;

6. Untuk memudahkan para pihak untuk menutup perjanjian (*finalize*) dan menyediakan bukti bagi telah adanya kesepakatan itu;
7. Untuk memastikan data/informasi yang ada belum pernah diubah/dirusak/*altered* sejak ia pertamakali dibuat (dengan kata lain disini ditekankan pada faktor *integrity* dari data tersebut);
8. Bahwa *digital signature* yang terdapat dalam pesan/data *messages* ini adalah dibuat dalam suatu jangka waktu yang terdapat didalam *certificate*. Jadi selama *certificate* itu masih *valid* (sah). *Digital signature* tersebut dibuat dengan menggunakan kunci privat, yaitu pasangan kunci dari kunci publik yang terdapat dalam *certificate* tersebut. Jangka waktu dari berlakunya *certificate* itu dapat dilihat di *Certificate Paractice Statement* (CPS) milik *issuer* dari *certificate* tersebut. Sedangkan untuk mengetahui apakah *certificate* tersebut masih *valid* atau tidak dapat dilihat di *Certificate Revocation List* (CRL). Keberadaan CPS dan CRL adalah sangat penting dalam proses penandatanganan suatu dokumen karena ia akan menentukan apakah dokumen tersebut *valid* atau tidak;
9. Untuk memudahkan pendokumentasian data dalam bentuk tertentu (*in tangible form*);
10. Bahwa *digital signature* tersebut adalah milik dari orang yang dianggap telah menandatangani (disini ditekankan pada prinsip otentisitas). Berdasarkan hal ini maka sangat penting untuk menjaga keberadaan kunci privat agar jangan sampai dipergunakan oleh orang lain yang tidak berhak. Apabila kunci privat itu hilang atau dicuri orang, maka *certificate* pasangannya harus segera di-*revoke*. Pemilik kunci yang asli mempunyai kewajiban untuk segera melaporkan peristiwa ini, karena ia dapat dimintai pertanggungjawaban atas penggunaan kunci yang tidak pada tempatnya;
11. Bahwa *digital signature* yang diterakan oleh pemiliknya, diterakan dengan kesadaran yang penuh dari penandatangan. Penandatangan tersebut harus bebas dari unsur tekanan, paksaan ataupun kekhilafan;

12. Untuk menunjang dilakukannya kontrol dan audit untuk kepentingan akuntansi, pajak dan ketentuan perundangan yang berlaku lainnya.

Data messages didalam SET mendekati atau hampir menyamai keunggulan oleh kontrak diatas kertas. *Data messages* ini menyediakan dukungan terhadap kehandalan (*realibility*) dan keutuhan (*unalterability*) yang dimiliki oleh kontrak diatas kertas.

Pasal 6 menekankan pada keuntungan dari sifat tertulis (*writing*) untuk maksud dan tujuan tertentu saja dan bukan secara umum. Pasal ini menekankan pada adanya alat bukti untuk kepentingan pajak dan peraturan perundangan yang berlaku lainnya. Pasal ini juga menekankan bahwa *data messages* tersebut harus dapat dibaca dan digunakan untuk berbagai tujuan.

Segala asumsi-asumsi maupun pernyataan yang telah disebutkan diatas (mengenai keberadaan *writing*) tidak mempunyai kekuatan hukum (*nullified*) apabila terdapat bukti secara teknis bahwa proses yang digunakan untuk memverifikasi *digital signature* secara teknis tidak *secure*. Para pihak yang hendak melakukan transaksi dengan menggunakan SET harus mempunyai *software* yang sudah memenuhi persyaratan (*compliance*) yang ditetapkan oleh *SET Root Certification authority*. Contoh dari program ini adalah *Vwallet* yang dibuat oleh Verifone. *Vwallet* ini digunakan untuk menyimpan kartu kredit *virtual* dan *purchse response*. Program ini telah memenuhi persyaratan *(compliance)* dari SET. Apabila kemudian *cardholder* menggunakan *software* selain yang telah dinyatakan *compliance* maka *digital signature* yang dihasilkannya dapat dikatakan tidak sah.

b. *Incorporate by Reference*

Pasal ini ditambahkan ke dalam *Model Law* oleh komisi dalam sesi ke-31 pada bulan Juni 1998. Pasal ini ditambahkan untuk memfasilitasi perkembangan hukum kontrak didalam *e-commerce*. Kontrak didalam *e-commerce* seringkali tidak memuat seluruh persyaratan-persyaratan dan kondisi-kondisi tertentu sebagai prasyarat sahnya kontrak tersebut secara utuh. Pasal ini dimaksudkan agar keberadaan dokumen-

dokumen yang mempunyai jenis seperti ini dapat mempunyai kekuatan hukum yang sama seperti jika seluruh persyaratan tersebut ada didalamnya.

Istilah *incorporate by reference* ini digunakan untuk menjelaskan suatu situasi dimana keabsahan suatu dokumen/*data messages* secara umum mengacu pada keberadaan suatu dokumen yang berada ditempat lain, dan bukan dengan melampirkan dokumen tambahan tersebut secara utuh. Berdasarkan hal tersebut diatas maka dapat disimpulkan maksud dari kalimat "*Incorporate by reference*" adalah:

Membuat suatu dokumen/*message* menjadi bagian yang tak terpisahkan dari dokumen yang lain, dengan jalan:

a. Mengidentifikasikan/memberitahukan tentang keberadaan message yang lain yang akan menjadi referensi (*to be incorporated*);
b. Menyediakan informasi yang cukup bagi penerima (*receiver*) sehingga ia dapat mengakses dan mendapatkan *message* yang akan digunakan sebagai referensi secara utuh, dan
c. Adanya persyaratan secara jelas yang mengatakan bahwa *message* tersebut adalah bagian dari referensi.

Penggunaan klausula *Incorporate by reference* ini terkait dengan penggunaan PKI (*Public Key Infrastructure*) didalam SET.

SET menggunakan *digital certificate* yang dikeluarkan oleh suatu *Certification Authority*. Keabsahan atau validitas dari *digital certificate* tersebut tergantung dari suatu dokumen yang lain (*Incorporate by reference*) dan juga dengan segala aturan-aturan yang dipunyai oleh *certification authority* tersebut. *Digital certificate* ini tergantung dari keberadaan CPS (*Certificate Practice Statement*). Dari CPS ini dapat diketahui segala hak dan kewajiban yang dipunyai pemilik *certificate* ini. Sedangkan masalah keabsahan atau validitas dari *certificate* ini tergantung CRL (*Certificate Revocation List*). CRL ini digunakan untuk mengetahui apakah suatu *certificate* masih berlaku/valid ataukah sudah di-*suspend* atau di-*revoke*.

Kontrak dalam *e-commerce* banyak bergantung pada klausula *incorporate by reference*. Keberadaan dokumen yang akan dijadikan acuan (*reference*) dalam dunia

elektronis dapat dipenuhi dengan digunakannya (tapi tidak terbatas oleh karenanya) *Uniform Resources Locators* (URLs)[56] dan *Object identifiers* (OIDs)[57].

URLs akan menyediakan "*hypertext links*" yang memungkinkan pengguna untuk menggunakan *pointing device* (misal: *mouse*) untuk "melompat" ke suatu alamat yang lain yang ditunjuk oleh *URLs* tersebut.

Masing-masing pihak didalam SET sebelum dan selama terjadinya transaksi akan selalu mengecek keabsahan dari *certificate* yang dimiliki oleh pihak yang lain. Pengecekan ini dilakukan dengan mengecek baik ke *root* ataupun melalui jaringan kartu kredit yang ada (*Visa* atau *Mastercard*). Apabila terdapat *certificate* yang tidak memenuhi syarat/rusak/*tempered* maka transaksi ini tidak dapat diselesaikan.

c. *Tandatangan (signature)*

Pasal 8 dari *Model Law* mengatur masalah keberadaan tandatangan didalam suatu kontrak. Pasal ini mengatur bahwa apabila terdapat suatu peraturan yang mensyaratkan perlu adanya suatu tandatangan (*signature*) maka ketentuan tersebut dapat dipenuhi oleh *data messages* apabila memenuhi persyaratan sebagai berikut:

1. Adanya suatu metode yang dapat digunakan untuk mengidentifikasikan si penandatangan. Terdapat juga indikasi bahwa orang tersebut telah membaca dan menyetujui isi dari perjanjian yang dibuatnya.
2. Metode tersebut dapat digunakan dalam perjanjian.

---

[56] URL adalah standar bagi penamaan alamat terhadap keberadaan suatu file/server di internet.

[57] *OIDs is a numeric value, composed of a sequence of integers, that's is unique with respects to all other OIDs. Object identifier used to define signature algorithm, certification policy, user defined alternatife name or user defined extension.*

Data messages yang digunakan didalam SET ditandatangani dengan menggunakan *hash function* yang menghasilkan *message digest* yang kemudian dienkripsi dengan menggunakan *private key* pengirim.

Message digest yang digunakan didalam PI dan OI akan memberikan bukti bagi keutuhan dari *data messages*. *Message digest* ini juga menunjukan bahwa OI/PI tersebut sifatnya adalah sudah *final* dan *binding*. Apabila PI dan OI tersebut diubah sejak ia pertamakali dibuat maka para pihak dapat dengan mudah mengetahuinya. Para pihak dapat mengetahuinya dengan cara membandingkan antara *message digest* yang sudah di-*encrypt* dengan kunci privat pengirim dengan *message digest* yang didapat dari menjalankan (*runs*) *hash function* terhadap *data message*. Hasil dari keduanya harus sama, apabila berbeda maka pasti *data messages* tersebut sudah pernah diubah atau dirusak (*altered*).

Penggunaan kunci privat yang digunakan untuk meng-*encrypt message digest* adalah bukti dari identitas penandatangan. Apabila penerima *data messages* dapat membuka tandatangan tersebut dengan kunci publik milik penandatangan maka terdapat bukti bahwa benar ia telah menggunakan kunci privatnya untuk menandatangani dokumen tersebut. Suatu pesan yang sudah di-*encrypt* dengan menggunakan kunci privat hanya dapat dibuka dengan menggunakan kunci publik pasangannya (*key pair*). Identitas dari pemilik kunci privat dan kunci publik adalah dapat dilihat dari *digital certificate* yang sudah divalidasi oleh *certification authority*.

Metode tandatangan yang digunakan didalam SET adalah *digital signature*. Sedangkan definisi *digital signature* sendiri adalah:

> " A transformation of message using an asymmetric cryptosystem such that a person having the ensured message and the ensurer's public key can accurately determine:
>
> a. Whether the transformation was created using the private key that corresponds to the signer's public key. And

b. Whether the signed message has been altered since the transformation was made.[58]"

Digital signature didalam PI dan OI adalah juga dikirmkan bersama dengan data messages yang dikirimkan. Dalam pengunaanya sehari-hari *digital signature* ini bisa saja dikirimkan secara terpisah atau disimpan dalam suatu tempat terpisah.

Proses verifikasi *digital signature* adalah proses yang menetukan dalam menetukan keabsahan dari *digital signature* tersebut. Proses ini dilakukan secara otomatis oleh *software* yang ada. Proses verifikasi ini dilakukan untuk menentukan:

a. apakah *digital signature* itu dibuat dengan menggunakan pasangan dari kunci privat;
b. apakah hasil dari *hash* yang baru (*newly computed hash*) adalah sama dengan *hash* yang didapat dari *digital signature* pada saat penandatanganan. (lihat gambar 2.6 dan langkah no. 10 dalam tabel 2.1)[59]

Pesan/kontrak yang sudah ditandatangani dengan menggunakan *digital signature* secara umum memiliki sifat yang hampir sama dengan kontrak yang dilakukan diatas kertas. Keunggulan ini didapat karena setiap perubahan (*alteration*) daripesan sejak pertamakali ia dibuat adalah dapat dengan mudah diketahui. Kontrak ini juga adalah sangat susah untuk untuk dipalsukan.

Sebuah *digital signature* seperti halnya sebuah tandatangan diatas kertas, sebenarnya adalah suatu mekanisme untuk melakukan otentifikasi. Tetapi, keduannya memiliki perbedaan yang penting terutama dalam hal pembuatan dan bagaimana cara

---

[58] International Chamber of Commerce, *GUIDEC* (*General Usance for International Digitally Ensured Commerce* (Paris: International Chamber of Commerce (ICC),1997).

[59]Information Security Committee, Section of Sciense and Technlogy, American Bar Association, *Digital Signature Guidelines*(Chicago: 1996) hal.12

melakukan verifikasi tandatangan diatas kertas dan digital signature mempunyai metode otentifikasi yang berbeda.

Sebelum menandatangani *data messages* seorang penandatangan akan diberikan kesempatan terlebih dahulu untuk melihat dan memperhatikan keseluruhan *message*. Penandatangan juga juga haruslah diberitahu dahulu bahwa ia akan menandatangani dokumen. Didalam SET, setelah memilih barang-barang yang akan dibeli *list* tersebut kemudian akan ditandatangani oleh *cardholder*. Apabila *data messages* tersebut tidak ditandatangani oleh *cardholder* maka PI tersebut tidaklah dapat diproses. Berdasarkan hal ini *cardholder* haruslah mempunyai keinginan untuk menandatangani data messages apabila ia kan membeli barang. *Digital signature* disini memiliki fungsi yang sama dengan tandatangan diatas kertas, yaitu penandatangan haruslah mempunyai keinginan untuk menandatangani PI.

d. *Surat Asli (Original) dan Salinannya (Copies)*

Berdasarkan *Model Law* salinan dari PI yang telah ditandatangani dengan menggunakan *digital signature* adalah sah, efektif dan mempunyai kekuatan pembuktian secara yuridis. Salinan dari surat asli (*data messages*) adalah mempunyai kekuatan pembuktian yang sama dengan *data messages* yang asli. Kekuatan pembuktian yang sama ini dikarenakan keduanya adalah terdiri dari bit-bit data dan bukanlah terdiri dari atom-atom kertas dan tinta, sehingga diantara keduannya adalah tidak terdapat perbedaan. Untuk dapat menetukan perbedaan antara dokumen asli/orisinil dengan dengan salinannya dapat dilakukan dengan cara melacak (*tracking*) sejarah pemrosesan (*processing*).

Perbedaan antara surat yang asli dengan salinannya merupakan hal yang penting dilihat dari sudut hukum. Hal ini didasarkan pada fakta bahwa didalam dunia komputer saat ini banyak tergantung pada proses penyalinan (*copies*) dalam menampilkan dokumen dan menjaga keutuhan pesan dan juga dalam proses pentransmisian data.

Kenyataannya, pada saat ini dalam dunia elektronis, suatu pesan hanya ada dalam bentuk salinan[60].

Suatu pesan pada saat ditandatangani secara elektronis (*digitally signed*) adalah berada didalam memori (*memory*) yang bersifat tidak stabil (*volatile*). Untuk menjaga keutuhan pesan ini satu-satunya cara adalah dengan membuat salinan dari isi (*content*) kedalam memori yang bersifat stabil yang ada dalam media yang lain (misal, *HardDisk*). Oleh karena itu kalau kita melihat secara teknis, dengan menggunakan teknologi yang ada pada saat ini suatu pesan yang otentik hanya ada di dalam memori komputer sampai dengan proses penandatangan itu selesai (*terminate*).

Model Law mengatur hal tentang orisinalitas pesan dalam Pasal 8. Pasal ini harus diartikan dalam konteks yang berbeda dengan pengertian kita selama ini mengenai keberadaan dokumen asli atau orisinil. Karena, *Addresse* (bisa *cardholder, Merchant, Payment Gateway*) selalu akan menerima salinan dari *data messages* yang asli[61]. Pasal ini digunakan dalam konteks dibutuhkan adanya suatu bukti akan keotentikan dari *message*. Pasal ini menyatakan bahwa suatu *message* dapat dikatakan asli/*original* apabila ia tidak pernah diubah-dibah atau dirusak (*tempered*) sejak ia pertamakali dibuat[62]. *Message* itu juga harus dapat diperlihatkan apabila terdapat kebutuhan akan isi dari pesan tersebut.

PI dalam SET adalah memenuhi ketentuan yang terdapat dalam pasal 8 *Model Law*. *Software* yang dimiliki oleh para pihak yang terlibat disini akan mengecek

---

[60] *Ibid.,*

[61] *Ibid.,*

[62] pasal 8 ayat 1 (a)

keutuhan pesan (*uniformity*) sebelum pesan tersebut diproses lebih lanjut. Apabila pesan tersebut pernah dirusak (*tempered*), maka proses itu akan dihentikan.

Purchase request yang dikirimkan oleh *cardholder* kepada *merchant* kepada *merchant* adalah terdiri dari OI, PI, *Digital envelope* dan juga *certificate* milik *cardholder*. OI dan PI telah ditandatangani terlebih dahulu oleh *cardholder* sebelum dikirimkan dengan menggunakan *dual signature*[63]. Apabila seseorang akan melakuakan pembayaran dengan menggunakan SET maka yang ia kirimkan tidak hanya *Payment Instruction* saja tetepi keseluruhan *purchase request*. Keberadaan OI, *Digital envelope* dan *digital certificate* adalah tidak mempengaruhi sifat *original* dari PI. PI disini tidak dapat dikatakan tidak original hanya karena terhadapnya telah ditambahkan OI, *digital envelope*. Tambahan-tambahan ini sifatnya tidak merusak keberadaan dari PI tersebut, ia hanya berfungsi untuk memungkinkan terjadinya transaksi itu saja. Dan tidak merusak keberadaan dan keutuhan dari PI. Pasal 8 ayat 3a dalam *Model Law* mengatakan bahwa kriteria terhadap keutuhan (*integrity*) dari suatu informasi dapat terpenuhi jika informasi tersebut adalah tetap utuh dan tidak pernah dirusak. Apabila terjadi penambahan terhadap informasi tersebut misalnya dengan adanya endosemen, *digital certificate* atau terdapat perubahan yang memang biasanya terjadi dalam hal komunikasi dan penyimpanan maka *message* tersebut tetap dianggap *original*.

Seperti telah dikemukakan diatas kriteria dari originalitas dalam PI adalah keutuhan (*integrity*) dari pesan. Aturan ini mengesampingkan adanya tambahan-tambahan terhadap *data messages* selama *data messages* ini masih tetap utuh.

---

[63] Visa and MasterCard, *op. cit.*,hal 59

Keberadaan aturan ini dapat kita asosiasikan dengan keberadaan endosemen dalam suatu kontrak. Endosemen ini tidak menyebabkan kontrak tersebut tidak *original* lagi. Penambahan-penambahan ini mungkin saja berupa *notarization*, *certification* dan lain sebagainya. Jadi pada saat terhadap PI ditambahkan *digital certificate* maka PI tersebut tetaplah dianggap *original*. Tambahan-tambahan atau lampiran tersebut akan dianggap seperti halnya ditambahkanya beberapa lembar kertas lampiran terhadap suatu dokumen "*original*". Atau dapat juga kita asosiasikan dengan menggangapnya sebgai amplop dan perangko yang akan kita gunakan apabila kita akan mengirimkan suatu dokumen "*original*".

Pasal ini menekankan pada pentingnya keutuhan (*integrity*) dari pesan untuk menunjukan keaslian/orisinalitas dari pesan tersebut.[64] Unsur-unsur yang harus dipenuhi agar dapat memenuhi ketentuan yang ada didalam pasal ini adalah adanya kriteria terhadap keutuhan *data messages*, adanya ketentuan tentang kriteria apa yang harus diperhitungkan dalam menentukan keutuhan suatu pesan.

Model Law memisahkan aturan mengenai "*writing*", "*original*", dan *signature* dalam pasal-pasal yang berbeda meskipun apabila kita lihat sepintas materi yang diatur adalah hampir sama. Pembedaan ini dikarenakan terhadap ketiga istilah ini masing-masing mempunyai konsep yang berbeda satu sama lain. Masing-masing istilah ini dalam kehidupan "sehari-hari" mempunyai makna yang berbeda, meskipun dalam penggunaanya dalam dunia elektronis makna yang terkandung adalah hampir sama.

e. *Saat Terbentuknya Kontrak*

Model Law mengatur saat terbentuknya kontrak berdasarkan prisip penawaran dan penerimaan (*offer and acceptance*). Prinsip ini adalah prinsip umum yang yang

---

[64] *loc. cit.*, Model Law, hal 26

digunakan dalam hukum kontrak internasional. Sedangkan mengenai bentuk dari kontraknya sendiri adalah bisa berbentuk *data messages* ataupun dalam bentuk lainnya dan tidak bergantung dalam bentuk tertentu. kedua prinsip ini adalah sesuai dengan prinsip yang terkandung dalam *United Nations Convention on International Sales of goods*.

Seorang pembeli dalam skim SET akan mengirimkan *offer* mengenai barang yang akan ia beli ke *merchant*. *Offer* yang ia kirimkan terdiri dari OI dan PI. OI dan PI ini akan ditandatangani secara ganda (*dual signature*)[65]. Maksud dari tandatangan ganda ini adalah, pembeli menyatakan maksud hendak membeli barang yang dijual *merchant* maka ia akan mengirimkan *offer* untuk melakukan pembelian (OI). PI berisi kewenangan bagi bank pembeli untuk mentransfer sejumlah uang sebagai pembayaran apabila *offer* yang dikirimkan diterima (*accept*) oleh *merchant*. Pembayaran hanya dapat diberikan apabila *merchant* meng-*accept offer* tersebut. Apabila *merchant* meng-*accept offer* tersebut maka ia akan meminta *payment authorization* ke *payment gateway*[66]. *Merchant* tidak harus melakukan otorisasi terlebih dahulu sebelum ia mengirimkan *purchase response* kepada pembeli. Apabila ia telah mengirimkan purchase response tersebut maka kontrak tersebut telah selesai. Penjual akan mengirimkan barang atau jasa yang ditawarkan kepada pembeli. Penjual akan mendapatkan pembayaran setelah ia melakukan proses *capture*.

Kontrak jual-beli ini selesai (*forming*) pada saat *merchant* mengirimkan *purchase response* kepada pembeli. *Purchase response* ini menandakan telah terjadinya

---

[65] *Ibid*., SET Book 1, hal 58

[66] *Ibid*., SET Book 1, hal 23

acceptance yang dilakukan oleh *merchant* atas *offer* yang ada. Saat terjadinya kontrak adalah pada saat *dispatch* dari *acceptance*.

Terdapat perbedaan yang menonjol antara penggunaan *digital signature* dalam suatu kontrak internasional dengan hukum kontrak internasional yang pada umumnya. *Digital signature* tidak akan memberikan bukti yang sama terhadap kedua belah pihak terhadap kontrak yang telah "ditandatangani". Didalam SET suatu *offer* dari pembeli yang berupa OI dan PI akan dibalas dengan *purchase response* dari *merchant*. Disini tidak terdapat bukti untuk *offeree* bahwa *offeror* telah menerima *acceptance* dari *offeree*, oleh karena itu dapat dikatakan hanya *offeror*lah yang mempunyai kontrak tersebut secara kontraktual. Hal ini tidak menjadi masalah secara ekonomi bagi kedua belah pihak selama pembeli membeli barang yang dibeli dan penjual menyerahkan barang yang dijual.

C. CERTIFICATION AUTHORITY

Penggunaan SET sebagai cara pembayaran di internet melibatkan berbagai pihak yang satu sama lainya secara geografis adalah berjauhan. Letak para pihak yang berjauhan ini menimbulkan masalah identitas dari para pihak (identifikasi). Secara hukum hal ini berhubungan dengan masalah kecakapan bertindak dari masing-masing pihak dalam melakukan suatu perbuatan hukum. Meskipun secara umum setiap orang yang sedah dewasa adalah cakap untuk bertindak namun untuk perbuatan-perbuatan hukum tertentu diperlukan adanya kualifikasi tertentu agar seseorang dapat disebut cakap. Sebagai contoh, seorang penerima *digital signature* (A) setelah melakukan verifikasi terhadap *digital signature* dan *public key* yang dikirim oleh pengirim (B) dapat merasa yakin bahwa pesan itu memang berasal dari B. Mereka dapat merasa yakin akan otentifikasi pesan/kontrak tetapi mereka (A, B) tidak tahu apakah keduannya adalah cakap dalam membuat kontrak pembayaran tersebut.

Certification authority salah satu fungsinya adalah menerbitkan *digital certificate*. *Digital certificate* berfungsi seperti layaknya tanda pengenal/KTP yang kita kenal

sehari-hari. Kecakapan seseorang bertindak adalah ditentukan dari *digital certificate* ini. *Digital certificate* adalah beranekaragam tergantung dari peruntukannya dan juga tingkat kecakapan yang dimiliki seseorang.

a. Digital certificate

SET menggunakan *digital certificate* untuk melakukan verifikasi terhadap identitas seseorang/badan hukum yang akan melakukan pembayaran dan juga pihak-pihak yang lain yang terlibat didalamnya. Software SET akan melakukan verifikasi terhadap identitas para pihak (pembeli, penjual, gerbang pembayaran, bank). setelah dilakukan verifikasi terhadap masing-masing pihak barulah dapat ditentukan apakah masing-masing pihak memang berwenang (cakap) melakukan transaksi atau tidak.

Sertifikat digital yang dipakai didalam SET adalah sertifikat milik pemilik kartu (*cardholder*), penjual (*merchant*), gerbang pembayaran (*payment gateway*), *acquirer*, penerbit kartu (*issuer*). *Digital certificate* yang digunakan dalam SET tidaklah berisi identitas seperti yang kita kenal selama ini (nama, alamat) *certificate* ini akan menghubungkan (*linking*) identitas (dalam arti luas) dengan integritas dari pesan. Penjual bahkan tidak mengetahui siapakah nama dari pembeli karena memang nama pembeli tidak ada didalam *certificate* tersebut. *Certificate* itu hanya menjelaskan bahwa memang *cardholder* tersebut adalah pemilik yang sah dari *credit card* yang digunakannya. Setiap transaksi yang dilakukan dengan menggunakan SET oleh karena itu bersifat anonim. ITU (*International Consultatife Committee on Telegraph and telephony*) sekarang dikenal sebagai *International Telecommunication Union*, mengeluarkan standar untuk otentifikasi terhadap data komputer dalam seri standar X.500[67]. Pada saat ini yang digunakan untuk melakukan otentifikasi bagi skim SET

---

[67] Marc Bronchoud, *A Survey of Public Key Infrastructure*, Xcert thesis.<http://www1.xcert.com/~marcnarc/PKI/thesis/thesis/preface.html>

adalah standar X.509 versi 3. X.509 v.3 adalah bagian dari seri standar X.500 yang dikeluarkan oleh ITU dan ISO.

Direktori yang disediakan oleh standar X.509 v.3 adalah menyediakan berbagai informasi yang penting dari diri seseorang. Informasi ini bisa berisi nama, tempat bekerja, pekerjaan jabatan, alamat dan lain sebagainya. Informasi-inforamsi inilah yang kan menentukan kecakapan seseorang dalam bertindak. Informasi yang terdapat dalam *digital certificate* ini adalah hampir-hampir sama dengan personifikasi yang kita temui dalam dunia nyata (*persoon, rechtpersoon*). Sertifikat yang dimiliki oleh seseorang adalah unik dan berbeda dengan sertifikat manapun didunia. Nama yang unik ini dinamakan sebagai *Distinghuised Name* (DN).

b. Catatan sipil/*Burgerlijk Stand*

Catatan sipil atau *burgerlijk stand* adalah suatu lembaga yang diadakan oleh penguasa, yang mempunyai maksud membukukan selengkap mungkin dan karena itu memberikan kepastian yang sebesar-besarnya tentang semua peristiwa penting/informasi mengenai status keperdataan seseorang. Hal-hal yang dicatata disini antara lain kelahiran, pengakuan, perkawinan, perceraian, kematian. Catatan sipil ini bersifat terbuka, sehingga setiap orang yang membutuhkan dapat mengakses atau meminta kutipan salinanya. Keberadaan status keperdataan seseorang ini adalah sangat penting dalam hal orang tersebut akan melakukan suatu hubungan keperdataan. Perkembangan teknologi saat ini (*e-commerce*/SET) membutuhkan keberadaan semacam catatan sipil ini yang senantiasa dapat diakses oleh publik secara *on-line*. Keberadaan catatan sipil ini yang dikeluarkan oleh suatu badan yang berwenang (*Authority*) akan memberikan identitas bagi orang tersebut di internet. Catatan sipil ini dapat dikembangkan dengan dengan menggunakan Standar direktori X. 509 sehingga dapat diakses secara *on-line*. Kutipan dari catatan sipil ini juga mempunyai kekuatan pembuktian (dalam *e-commerce* dikenal dengan menggunakan istilah *incorporate by reference*) sehingga catatan sipil ini pada prinsipnya dapat digunakan untuk berbagai macam transaksi.

D. PERMASALAHAN HUKUM

SET mempunyai berbagai keunggulan dibandingkan sistem pembayaran di internet yang lainnya. SET termasuk sistem pembayaran yang aman, SET juga memiliki keunggulan dalam hal *Authenticity*, *integrity*, *confidentiality* dan *non-repudiation*. Keunggulan-keunggulan yang dipunyai oleh SET ini juga dapat menjadi kekurangan bagi sistem ini dibandingkan sistem pembayaran di internet yang lain (terutama dengan sistem pembayaran *Mail Order/Telephone Order*) kelemahan ini terutama didalam masalah *non-repudiation*.

Fungsi *non-repudiation* terutama diperuntukan untuk memberikan kepastian bagi para pihak yang terlibat dalam bertransaksi di internet untuk tidak dapat membantah (*denial*) bahwa ia tidak melakukan perbuatan tersebut. Apabila seorang *cardholder* melakukan pembayaran dengan menggunakan SET maka ia tidak dapat membantah bahwa ia tidak melakukan transaksi tersebut. Fungsi ini sekilas mempunyai keunggulan, yaitu memberikan kepastian bagi pedagang untuk mendapatkan pembayaran atas barang yang dijualnya. Kelemahan atau permasalahan hukumnya disini adalah lemahnya perlindungan hukum bagi konsumen. Lemahnya posisi konsumen adalah pada saat kartu kreditnya hilang atau telah dipalsukan oleh orang lain. Apabila kemudian kartu itu dipergunakan oleh orang lain maka pemilik kartu kredit yang asli tidak dapat membantah bahwa ia tidak mempergunakan kartu kredit tersebut. *Cardholder* harus membayar setiap transaksi yang terjadi meskipun ia tidak melakukan transaksi tersebut. Didalam transaksi *Mail Order/Telephone Order* (MOTO), posisi konsumen lebih kuat. *Cardholder* dapat membantah telah melakukan suatu transaksi atau menggunakan kartu kreditnya untuk melakukan pembayaran. *Cardholder* tidak harus membayar atas transaksi yang tidak pernah ia lakukan. *Merchant* mempunyai kewajiban untuk membuktikan bahwa memang *cardholder* telah melakukan transaksi di tokonya. Jadi, dalam transaksi MOTO *cardholder* mendapat perlindungan hukum yang lebih dibandingkan dengan transaksi yang menggunakan SET.

Perkembangan *e-commerce* dan sistem pembayaran di internet menimbulkan berbagai permasalahan hukum dibidang perpajakan, terutama masalah mengenai bagaimana memungut pajak atas transaksi yang terjadi melalui *e-commerce*. Kesulitan terbesar yang dihadapi oleh aparat pajak adalah adalah bagaimana dapat mengumpulkan/mengambil data untuk kepentingan perpajakan dari *internet traffic*. Kesulitan ini terutama karena didalam internet terdapat berbagai macam data yang ditransmisikan melalui internet. Jenis informasi yang harus didapatkan untuk keperluan perpajakan adalah masalah yang berkaitan dengan apakah terdapat suatu perbuatan hukum/transaksi yang dapat dikenai pajak dan bagaimanakah cara suatu otoritas/negara dapat mengetahui bahwa terdapat warganegaranya yang dapat dikenai pajak.

SET menggunakan *encryption* dalam mentransmisikan data-data yang diperlukan dalam melaksanakan transaksi. Teknologi *encryption* ini akan menghalangi pihak ke-3 (dalam hal ini pemerintah) untuk mendapatkan informasi yang penting dalam bidang perpajakan. Perkembangan yang terakhir pada saat ini adalah dikembangkannya protokol baru yang bernama *Internet OpenTrading Protocol* (IOTP) yang dibuat dan diperkenalkan oleh *Internet Engineering Taskforce* (IETF)[68]. Protokol ini memungkinkan pihak pemerintah untuk memonitor data-data yang penting untuk keperluan perpajakan. SET dan juga sistem pembayaran di internet lain (Mondex, Secure channel, Cyber Coin) juga mendukung protokol ini. Beberapa negara di dunia pada saat ini juga sedang berusaha menerapkan protokol ini, misalnya Kanada dan Jepang[69]. Pengembangan protokol baru ini seharusnya juga dapat diantisipasi oleh aparat perpajakan di Indonesia mengingat besarnya potensi pajak yang bisa didapatkan

---

[68] Kabich, Volker, *Law and Technology Convergence - Tax* (ECLIP:1999), hal.11. <http://www.jura.uni-muenster.de/eclip>

[69] *Ibid.,*

dari *e-commerce*. Pemerintah haruslah menyiapkan aparat dan juga perundang-undangan yang memadai dalam mengansipasi perkembangan dibidang perpajakan ini.

BAB IV

PENUTUP

A. KESIMPULAN

Dari uraian-uraian yang telah disampaikan pada bab-bab sebelumnya, penulis mengambil beberapa kesimpulan sebagai berikut:

1. SET adalah sebuah skim (*scheme*) dalam *Internet Payment System*, yang dikembangkan pertama kali oleh Visa dan Mastercard. Skim ini dibuat untuk memenuhi kebutuhan akan adanya transaksi pembayaran dengan menggunakan kartu kredit di internet yang aman. SET menggunakan *public key encryption* dalam meng-*encrypt Payment Instruction (PI)* dan *Order Instruction (OI)*. Penggunaan teknik ini akan memberikan kekuatan hukum bagi *data messages* (PI dan OI) sehingga akan memberikan perlindungan hukum bagi *cardholder*.
2. SET menggunakan kombinasi antara fungsi hash (*hash function*) dan *public key encryption* dalam menandatangani *Payment Instruction* (PI) dan *Order Instruction* (OI). Penggunaan *hash function* dan *encryption* ini akan menjamin keutuhan, keotentikan dan kerahasiaan dari PI dan OI. PI dan OI ini tidak akan dapat dibaca dan diubah oleh orang lain yang tidak berhak. SET menggunakan *hash function* yang akan menghasilkan 160-bit *message digests*. *Message digests* sepanjang ini akan memberikan perlindungan terhadap keutuhan dari PI dan OI. Kemungkinan terdapat dua buah *message digests* yang sama adalah satu diantara sepuluh pangkat 16. SET menggunakan *public key encryption* dengan panjang 512 bit. Kunci sepanjang ini pada tahun 1999 dengan menggunakan komputer seharga US $ 100,000,00 dengan menggunakan metode *brute force attack* baru dapat diuraikan setelah 10.000 tahun. Dengan mengkombinasikan keduanya (*hash function* dan *public key encryption*) akan meningkatkan keamanan dari SET. SET mengatur bahwa sebelum para pihak melakukan hubungan hukum maka mereka harus

terlebih dahulu mengecek identitas dari para pihak. Verifikasi dari identitas para pihak adalah dengan cara mengecek digital certificate yang dipunyai oleh para pihak. Jika *digital certificate* tersebut sah/valid barulah para pihak dapat melakukan hubungan hukum. Kontrak pembayaran dalam SET dibuat dalam bentuk digital signature.

3. *Uncitral Model Law on Electronic Commerce* mengatur tentang penggunaan *data messages* dan pemberian kekuatan hukum terhadap suatu *data messages*. Kontrak didalam *e-commerce* yang menggunakan *data messages* harus memenuhi berbagai persyaratan yang ada didalam *Model Law* sehingga dapat mempunyai kekuatan hukum. SET menggunakan *data messages* yang telah ditandatangani dengan menggunakan *digital signature*. Penggunaan *digital signature* ini membuat *data messages* yang ada dalam skim SET mempunyai kekuatan hukum seperti yang diatur dalam *Model Law*.
4. Hingga saat ini belum ada aturan hukum di Indonesia yang secara khusus mengatur keberadaan *data messages* dan penggunaan *digital signature*. Meskipun demikian BW tidak mengharuskan kontrak dalam suatu bentuk tertentu. Jadi, apabila suatu kontrak dibuat dalam bentuk *data messages* dan ditandatangani dengan menggunakan *digital signature*, maka berdasarkan BW kontrak tersebut tetap mempunyai kekuatan hukum. Keberadaan Catatan Sipil/*Burgerlijk Stand secara* prinsip mirip dengan keberadaan *Certification Authority*. *Certification authority* adalah suatu otoritas yang akan menerbitkan suatu *digital certificate* milik seseorang. *Digital certificate* ini berisi identitas dan juga kecakapan bertindak dari orang tersebut. *Digital certificate* ini akan ditempatkan didalam suatu direktori publik sehingga setiap orang dapat dengan mudah mengetahui identitas dan kecakapan dari orang lain.
5. Permasalahan hukum yang timbul dari penggunaan SET antara lain adalah kurangnya perlindungan hukum bagi seseorang *cardholder*. Kurangnya perlindungan hukum ini terutama pada saat kartu kredit yang dimilikinya digunakan oleh orang yang tidak berhak. Sesuai dengan sifat *non-repudiation* dari

digital signature maka orang tersebut tidak dapat mengklaim ia tidak pernah melakukan transaksi tersebut. Masalah berikutnya yang timbul adalah yang berkaitan dengan masalah perpajakan. Adalah sangat sukar untuk memungut pajak dalam transaksi pembayaran yang menggunakan SET karena ia menggunakan *encryption* yang kuat, yang tidak memungkinkan pihak ketiga mengetahui isi dari pesan yang telah di-*encrypt* tersebut. Penggunaan *encryption* ini disatu sisi akan meningkatkan keamanan tapi di sisi lain akan menyulitkan pihak yang berwenang untuk memungut pajak.

B. SARAN

1. Mengingat pada saat ini belum ada peraturan di Indonesia yang mengatur secara khusus mengenai keberadaan dokumen elektronik dan *e-commerce* maka penulis menyarankan agar segera dibuat peraturan perundangan mengenai dokumen elektronis. Aturan mengenai dokumen elektronis dan *e-commerce* ini hendaknya menganut prinsip *technology neutrality*. Maksud dari prinsip ini adalah peraturan ini tidak hanya mengatur tentang penggunaan suatu teknologi tertentu saja tetapi juga mengakomodir kemungkinan penerapan teknologi yang lain. Selain itu agar suatu peraturan perundangan tidak cepat berubah karena adanya perkembangan teknologi namun tetap dapat mengakomodir perkembangan teknologi. Hal ini penting diperhatikan karena teknologi komputer/internet sangat cepat berubah.
2. Keberadaan internet dan kegiatan bisnis yang dilakukan didalamnya harus dicermati oleh para pihak yang berwenang. Dengan adanya suatu peraturan perundangan yang mengatur kegiatan bisnis melalui internet diharapkan dapat memacu pertumbuhan bisnis internet di Indonesia. Bisnis melalui internet ini selain mengandung berbagai kemungkinan bisnis yang baru, juga memunculkan berbagai permasalahan hukum yang baru. Adanya suatu peraturan perundangan mengenai hal ini akan memberikan kepastian hukum dan ketenangan bagi para pelaku bisnis.