METODE KEAMANAN DATA DALAM *E-COMMERCE*

Oleh: **Frieyadie**

ABSTRAK

Sistem Keamanan dalam E-Commerce merupakan menjadi perhatian yang sangat serius. Karena dengan e-commerce semua transaksi yang dilakukan dengan media transmisi yang mudah di "bajak" oleh pihak-pihak yang tidak berhak. Kejahatan di dunia maya sangat sering terjadi, mulai dari penipuan, penyalahgunaan kartu kredit sampai dengan penghancuran sistem. Oleh karena itu untuk menjaganya diperlukan suatu strategi dan teknologi yang dapat melindungi paket-paket yang dikirimkan.

I. PENDAHULUAN

Electronic Commerce (E-Commerce) secara umum merupakan kegiatan bisnis (perniagaan atau perdagangan) atau jasa yang berhubungan erat dengan konsumen (*Consumers*), Manufaktur, *Internet Service Provider* (ISP) dan Pedagang Perantara (*Intermediateries*) dengan menggunakan media elektronik. Dalam hal ini media elektronik utama dengan menggunakan *internet*.

Melakukan transaksi menggunakan cara elektronik memberikan beberapa manfaat diantaranya adalah sebagai berikut :

a. Biaya informasi lebih murah.
b. Akses 24 jam.
c. Kesempatan perluasan pasar lebih terbuka.
d. Menurunkan biaya penciptaan, proses, distribusi, penyimpanan.
e. Mengurangi biaya komunikasi.
f. Memperkaya komunikasi kepada pembeli daripada secara tradisional.
g. Pengiriman secara digital untuk produk seperti gambar, dokumen, *software*.
h. Meningkatkan fleksibilitas lokasi.

Untuk itu kita butuh untuk melindungi segala bentuk transaksi yang akan dilaksanakan di *internet*.

II. PEMBAHASAN

STRATEGI MELINDUNGI TRANSAKSI *E-COMMERCE*

Ada beberapa strategi yang dapat digunakan untuk melindungi transaksi dengan *e-commerce*, yaitu:

Kriptografi (*Cryptography*).

Menurut tulisan yang diambil dari *website*. http://en.wikipedia.org/wiki/Cryptography kriptografi adalah suatu proses pengkodeaan data mentah, menjadi data yang tersamar yang dikirimkan oleh pengirim yang dapat disampaikan oleh penerima dengan aman dengan teknik pemetaan tertentu. Penggunaan kriptographi dalam *e-commerce* atau penggunaan *internet* telah banyak membantu dalam menyelesaikan masalah keamanan (*security*). Kriteria keamanan yang dipergunakan dalam kriptographi adalah:

1. Kerahasiaan (*Confidentiality*)
   Kerahasiaan disini dimaksudkan adalah suatu data atau paket data tidak diperbolehkan dibaca atau diketahui oleh orang lain atau pihak lain yang tidak berkepentingan.
2. Otensitas (*Authenticity*)
   Otentisitas merupakan proses verifikasi terhadap identitas pengirim data atau paket data.
3. Integritas (*Integrity*)

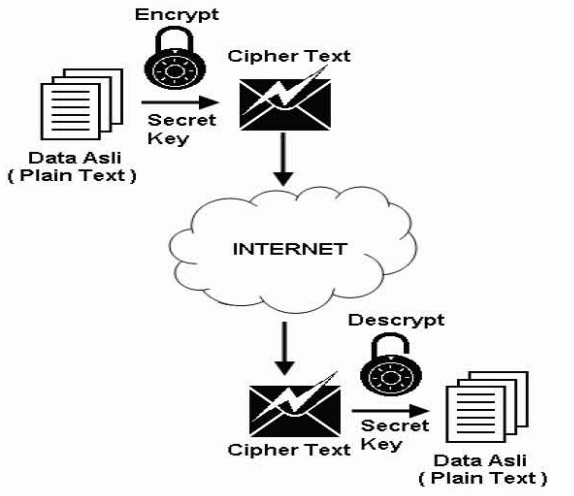
Maksud integritas disini adalah keutuhan data atau paket data yang dikirimkan oleh pengirim dan penerima data atau paket data yang diterimanya benar-benar utuh dan tidak dimanipulasi atau diubah.

4. Tidak Dapat Disangkal
   Maksud dari tidak dapat disangkal bahwa setiap pengiriman data atau paket data, pengirim tidak bisa menyangkal bahwa tidak pernah mengirim data atau paket data tersebut.

Data asli dalam kriptographi disebut dengan *plaintext*. *Plaintext* disini dapat berupa data gambar, video, teks dan sebagainya. Suatu data atau paket data yang ditransformasi oleh kriptographi disebut dengan *ciphertext*. Proses pengembalian dari tranformasi data dalam bentuk *ciphertext* ke bentuk semula disebut dengan deskripsi (*decryption*).

Jenis kriptographi yang paling umum digunakan adalah Algoritma Simetris (*Symmetric Algorithm*).

Kunci yang dibuat untuk me-*encrypt* sama dengan kunci yang digunakan untuk membuka atau *descrypt*.



Gambar II.1

Proses *Encryption* dan *Descryption*

Contoh penggunaan Algoritma Simetris adalah *Data Encryption Standard* (DES). Kelemahan dari proses ini diantaranya adalah :

a. Kunci yang dipergunakan yaitu sama, jadi antara pengirim dan penerima haruslah saling percaya.
b. Jika dua atau lebih orang memiliki kunci yang sama, maka mungkin salah satu orang yang memegang kunci tersebut bisa mencuri atau mendeskripsikan data tersebut.
c. Penerima data atau paket data belum tentu yakin bahwa si pengirim data atau paket data adalah orang yang sebenarnya, bisa saja orang lain yang memakai nama orang yang bersangkutan.

Algoritma Kunci Publik (*Public-Key Algorithm*)

Menurut tulisan yang diambil dari *website*, http://en.wikipedia.org/wiki/Public_key_algorithm, Algoritma Kunci Publik disebut juga dengan algoritma asimetris (*Asymmetric Algorithm*) yaitu algoritma yang menggunakan kunci yang berbeda pada saat melakukan enkripsi dan melakukan deskripsi. Pada saat melakukan enkripsi dan mendistribusikan ke umum atau publik, algoritma yang digunakan adalah kunci publik.

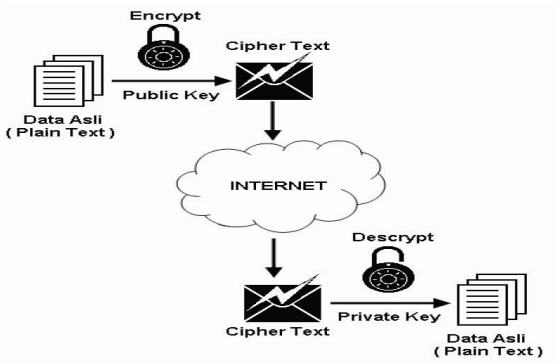
Paket data yang diterima akan dibuka atau deskripsi dengan mengunakan algoritma kunci *private*. Antar kunci publik dan kunci *private* mempunyai hubungan secara matematis, dapat diartikan bahwa seseorang yang mempunyai kunci publik tidaklah dapat membuat kunci *private* dan kunci publik tersebut. Metode yang digunakan pada algoritma asimetris adalah sebagai berikut :

1. RSA (*Rivest, Shamir, Adleman*).
2. DH (*Diffe, Hellma*).
3. PGP (*Pretty Good Privacy*).
4. *El Gammal.*
5. DSA (*Digital Signature Algorithm*).

6. *Schnoor.*

Dengan adanya Algoritma Kunci Publik (*Public-Key Algorithm*), kekurangan-kekurangan yang ada pada *Symmetric Algorithm* dapat teratasi, dan solusi yang dapat diambil yaitu :

1. Setiap orang penerima atau pengirim hanya mengingat kunci pribadinya saja.
2. Algoritma bekerja berdasarkan pasangan kuncinya saja. Sehingga bila seseorang memiliki kunci yang sama akan tetapi pasangan kuncinya berbeda, maka tidak dapat mendeskripsikan data atau paket data orang lain.
3. Masalah autentifikasi dapat teratasi, bahwa data, hanya dapat dibuka oleh orang yang memiliki pasangan kunci tersebut.



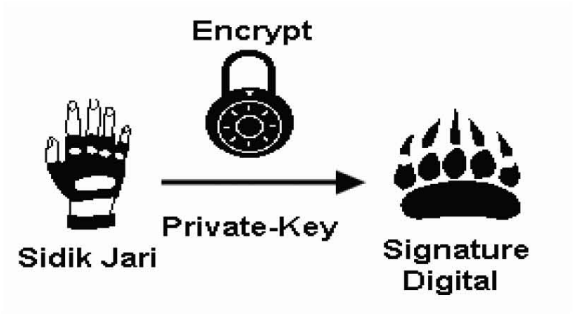
Gambar II.2 Proses *Private-Key* dan *Descryption* pada *Asymmetric Algorithm*

Kelemahan dari *Asymmetric Algorithm* ini adalah pada pelaksanaan secara teknis memakan waktu untuk melakukan pengkodeaan dengan kunci publik.

Tanda Tangan Digital (*Digital Signature*)

Tanda tangan digital merupakan tanda tangan yang dibuat secara elektronik, dengan jaminan yang lebih terhadap keamanan data dan keaslian data, baik jaminan tentang identitas pengirim dan kebenaran dari data atau paket data tersebut.

Dalam tulisan yang berjudul "*Digital Signature*", diambil dari *website* http://en.wikipedia.org/wiki/Digital_signature, bahwa tanda tangan digital dapat menggunakan Algoritma Simetris atau Algoritma Kunci-Publik. Penggunaan Algoritma Simetris, akan menggunakan perantara atau *arbitrator* pada pembuatan tanda tangan digital yang aman, akan tetapi untuk saat ini pembuatan tanda tangan digital sudah menggunakan Algoritma Asimetris. Pembuatan tanda tangan digital dengan menggunakan Algoritma Kunci-Publik banyak metode yang bisa digunakan diantaranya RSA yang menggunakan kunci-*private* atau kunci-publik untuk melakukan enkripsi.

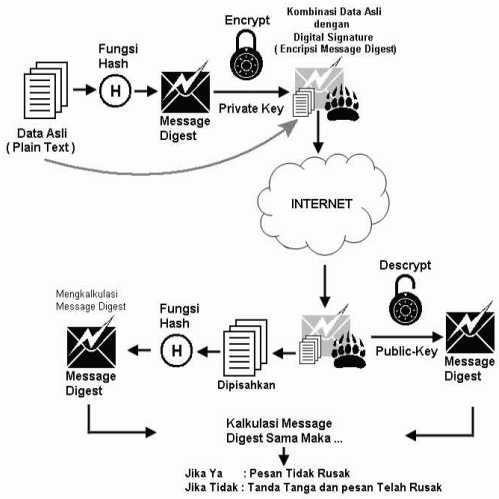


Gambar II.3 Pembuatan Tanda Tangan

Biasanya Tanda tangan digital dikombinasikan dengan Fungsi *Hash*, dengan tujuan untuk mengefesiensikan kerja dalam penandatanganan data. Pada *Digital Signature* dengan Fungsi *Hash* langkah yang diambil yaitu :

1. Data Asli atau Paket Data dikodekan dengan menggunakan Fungsi *Hash*. Misalnya menggunakan Fungsi *Hash* 16 *Byte*, yang hasilnya dinamakan *Message Digest*.
2. *Message Digest* ini kemudian di enkripsi dengan menggunakan *private-key*, yang hasilnya berupa *Digital Signature*.

3. *Digital Signature* ini yang kemudian digabungkan dengan teks dokumen asli.
4. Penerima akan melakukan proses autotenfikasi.
5. Memisahkan data asli dengan *Digital-Signature*, yang menyertainya.
6. Melakukan proses fungsi *Hash* terhadap data asli sehingga didapatkan *Message Digest*.
7. Melakukan proses deskripsi terhadap *digital-signature* dengan menggunakan kunci publik.
8. Membandingkan hasil aktivasi deskripsi dengan hasil fungsi *digest*. Jika Data tersebut identik maka, maka data dan *digital-signature* yang diterima adalah otentik. Jika tidak, maka terdapat 3 (tiga) kemungkinan :
   a. Data yang dikirimkan telah mengalami perubahan dari segi isi.
   b. *Digital-Signature* telah mengalami modifikasi.
   c. Data dan *Digital-Signature* telah mengalami perubahan dan tidak asli lagi.



Gambar II.4 Proses *Digital Signature* dan *Fungsi Hash*.

Manfaat Tanda Tangan Digital

Ada tiga pertimbangan umum untuk penerapan suatu tandatangan digital pada komunikasi :

a. Authetentication

Public-Key Crypto Systems mengijinkan *encryption* dari suatu pesan dengan *user private-key*. Pesan itu sendiri tidak perlu dimasukkan *ciphertext*. Jika *Hash* menghasilkan dokumen dan kemudian dilindungi *via encryption*, dokumen tidak bisa diubah bagaimanapun juga tanpa mengubah *hash* yang berkesesuaian, jika mutu algoritma digunakan secara baik, maka akan menjadi hal yang sungguh menyulitkan. Dengan *decrypting hash* dapat menggunakan pengiriman kunci publik, dan memeriksa hasil terhadap suatu *hash* yang baru menghasilkan *plaintext* yang dimaksud, penerima dapat mengkonfirmasikan bahwa *encryption* dilaksanakan dengan pengiriman kunci pribadi, dan pesan tersebut belum dirubah.

b. Integrity

Kedua belah pihak akan selalu yakin pesan belum dirubah selama transmisi. Enkripsi pesan membuat pihak ketiga sulit untuk membaca pesan tersebut, tetapi pihak ketiga tetap mampu mengubah pesan itu, mungkin dengan jahat, benar-benar membaca pesan itu. Contoh adalah *homomorphism Attack* yaitu mempertimbangkan suatu bank yang mengirimkan instruksi dari kantor cabang kepada kantor pusat, didalam format pesan tersebut contoh (a, b) di mana a adalah nomor *account*-nya atau rekeningnya dan b adalah jumlah nominal *acount* tersebut.

c. Non-Repudiation

Dalam konteks *cryptographic*, Kata *Repudiation* mengacu pada tindakan dalam menyangkal tanggung jawab untuk pada suatu pesan. Penerima pesan boleh meminta dengan tegas pengirim harus menyertakan *signature* dalam permintaan *repudiation* kemudian

yang lebih sulit, sejak penerima dapat menunjukkan pesan (*message*) yang ditandatangani kepada pihak ketiga untuk menguatkan suatu klaim seperti asal nya.

Bagaimanapun, hilangnya kendali pada suatu pemakaian kunci pribadi akan berarti bahwa pemakai tersebut merupakan orang yang dicurigai. Terlihat bahwa hilangnya kendali seperti itu telah terjadi bukan suatu masalah kriptographi, tetapi suatu kesalahan manusia dan belum terungkap.

Ada beberapa pertimbangan pada *digital signature*, yaitu :

1. Untuk Efisiensi
   Tandatangan akan jauh lebih lebih pendek dan begitu menghemat waktu karena pemilahan-pemilahan biasanya banyak dan lebih cepat.
2. Dokumen dimaksudkan untuk dibaca oleh orang yang lain.
   Seperti : ijazah, surat kelahiran, identitas sertifikat, lisensi pengemudi, suatu kontrak yang menetapkan kepemilikan sesuatu barang, dan lain-lain. Dokumen ini akan berada di *cleartext*, tetapi pada saat disertakan pada tandatangan digital dapat digunakan untuk memverifikasi bahwa itu yang bukan diubah.
3. Untuk integritas.
   Tanpa adanya fungsi *hash*, teks harus dipisah-pisahkan dalam suatu blok dengan suatu ukuran yang lebih pendek dibanding panjang kunci pribadi. Kemudian masing-masing blok harus ditandatangani dan dikirim kepada penerima. Bagaimanapun, penerima dari blok ditandatangani adalah tidak mampu mengenali jika satu atau lebih blok telah dihapus sepanjang transmisi.

Penerapan *Public-Key Digital Signature*

Public-Key Digital Signature secara terencana dipercayakan pada *Public-Key Cryptograpy*. Didalam *Public-Key Cryptograpy* masing-masing pemakai memiliki sepasang kunci yaitu satu *public* dan satu *private*. Kunci *Public* didistribusikan secara bebas dan kunci *private* tetap dirahasiakan oleh pemakai, kebutuhan lainnya adalah untuk memperoleh *private-key* harus memiliki perhitungan yang tidak mungkin mengirimkan *public-key* dari suatu *public-key*. Secara umum, *digital signature* meliputi 3 (tiga) algortima, yaitu:

1. *A key generation algorithm*
2. *A signing algorithm*
3. *A verification algorithm*

Beberapa masalah yang mungkin timbul dari sistem *digital signature* ini terkait dengan sistem hukum yang sudah ada. Pada banyak negara, disyaratkan bahwa suatu transaksi harus disertai dengan bukti tertulis, dengan pertimbangan kepastian hukum.

Permasalahan yang ada pada *Digital-Signature* yaitu, bagaimana sebuah dokumen elektronik yang ditandatangani dengan sebuah *digital signature* dapat dikategorikan sebagai bukti tertulis ?

Di Inggris, bukti tertulis haruslah berupa tulisan, ketikan, cetakan, litografi (*lithography*), fotographi, atau bukti-bukti yang mempergunakan cara-cara lain, yang dapat memperlihatkan atau mengolah kata-kata dalam bentuk yang terlihat secara kasat mata. Definisi dari bukti tertulis itu sendiri sudah diperluas hingga mencakup juga "*telex*, telegram, atau cara-cara lain dalam telekomunikasi yang menyediakan rekaman dan perjanjian" (*UNCITRAL Model Law on Internatinal Commercial Arbitration, art.7* (2)).

Dokumen elektronik yang ditandatangani dengan sebuah *digital signature* dapat dikategorikan sebagai bukti tertulis. Apabila, terdapat suatu prinsip hukum yang menyebabkan

sulitnya pengembangan penggunaan dan dokumen elektronik atau *digital signature*, yakni adanya syarat bahwa dokumen tersebut harus dapat dilihat, dikirim dan disimpan dalam bentuk kertas. Masalah lain yang dapat timbul berkaitan dengan dokumen elektronik dan *digital signature* ini adalah masalah cara untuk menentukan dokumen yang asli dan dokumen salinan.

Berkaitan dengan hal ini sudah menjadi prinsip hukum umum bahwa :

a. Dokumen asli harus dalam bentuk perjanjian tertulis yang ditandatangani oleh para pihak yang melaksanakan perjanjian.
b. Dokumen asli hanya ada satu dalam setiap perjanjian.
c. Semua reproduksi dari perjanjian tersebut merupakan salinan.

Sertifikat Otoritas (*Certificate Autority*)

Sertifikat Otoritas merupakan pihak ketiga yang bisa dipercaya (*Trust Thrid Parti*/TTP). Sertifikat Otoritas yang akan menghubungkan kunci dengan pemiliknya. TTP ini akan menerbitkan sertifikat yang berisi identitas seseorang dan juga kunci *private* dari orang tersebut. Tugas dari sertifikat otoritas adalah :

1. Membuat kunci publik atau *private* miliknya sendiri.
2. Melakukan verifikasi terhadap identitas seorang calon pelanggan yang hendak meminta sertifikat dari sertifikat otoritas tersebut.
3. Pelanggan melakukan penyerahan kunci publiknya kepada sertifikat otoritas.
4. Sertifikat Otoritas mengecek kunci tersebut pasangan dari kunci *private* yang dimiliki calon pelanggan.
5. Jika keseluruhan persyaratan terpenuhi maka Sertifikat Otoritas akan menerbitkan sebuah sertifikat digital atas nama orang tersebut,

Digital Serficate berisikan kunci duplikat dari kunci-publik pelanggan dan juga identitas dari pelanggan.

Secure Socket Layer (SSL)

Secure Socket Layer (SSL) merupakan suatu protokol yang membuat sebuah pipa pelindung antara *browser cardholder* dengan *merchant*, sehingga pembajak atau penyerang tidak dapat menyadap atau membajak informasi yang mengalir pada pipa tersebut. Pada penggunaannya SSL digunakan bersamaan dengan protokol lain, seperti HTTP (*Hyper Text Transfer Protocol*), dan *Sertificate Autority*. Penggunaan *Sertificate Autority* ini ditujukan untuk meningkatkan pengamanan terhadap pembajak atau penyadap informasi yang terdapat pada pipa SSL. Pembajak yang melakukan penyadapan informasi bisa melakukan pengubahan-pengubahan informasi dengan cara menukar *public-key chardholder* dan *merchant* dengan *public-key* pembajak.

Menurut tulisan yang berjudul *Transport Layer Security*, dari *website* http://en.wikipedia.org/wiki/TranportLayerSecurity, SSL Melibatkan tiga tahapan dasar, yaitu :

1. *Peer Negotiation For Algorithm Support.*
2. *Public Key Encryption base key exchange and certificate base authentication.*
3. *Symmetric Cipher base traffic encryption.*

Penggunaan *Symmetric-Key* yang digunakan pada SSL, untuk membungkus data asli, misalnya data kartu kredit. *Symmetric-Key* yang dipergunakan pada *web browser*, pada umumnya menggunakan RC4 dan DES (*Data Encryption Standard*). Teknologi Enkripsi berkekuatan tinggi (*Strong Encryption*) yang ada sekarang yaitu RSA 1024 *bit* dan RC4/DES 128 *bit*. *Web browser* yang menggunakan teknologi enkripsi

berkekuatan tinggi diantaranya *Microsoft Internet Explorer (IE)* dan *Netscape Communicator (NC)*.

Berikut contoh membuat SSL dengan SSL *Manager,* dengan SSL *Manager* ini memungkinkan kita untuk membuat SSL *Certificate*, *Signing Request, SSL Key*.

Didalam pengaplikasiannya SSL berjalan pada lapisan di bawah protokol aplikasi seperti HTTP, FTP, SMTP dan NNTP, dan di atas TCP atau UDP yang berhubungan dengan protokol, yang mana membentuk bagian dari TCP/IP protokol. Selain itu dapat menambahkan keamanan untuk protokol manapun yang menggunakan koneksi dan dapat dipercaya (seperti TCP), hal yang yang paling umum yaitu digunakan pada HTTP untuk membentuk HTTPS. HTTPS digunakan untuk menjamin keamanan *World Wide Web* untuk aplikasi seperti perdagangan elektronik. Hal itu menggunakan *public-key certificate* untuk memverifikasi identitas *end-points*.

Protocol SSL dan TLS menggunakan *cryptography public-key* dan sertifikat *publik key* untuk memastikan identitas dari pihak yang dimaksud. Sejalan dengan peningkatan jumlah *client* dan *server* yang dapat mendukung TLS atau SSL alami, dan beberapa masih belum mendukung. Dalam hal ini, pengguna dari *server* atau *client* dapat menggunakan produk *standalone*-SSL seperti halnya *Stunnel* untuk menyediakan enkripsi SSL

Gambar II.5. SSL *Manager*

a. Berikut Adalah hasil *generate* pembuatan *Private Key, SSL Key* dengan *Private Key* 1024 *bit* dengan menggunakan SLL *Manager*

SSL *Key Generated Key*

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC/mnJFiqbb3GO/GX3hKJfLhaHyqAW5yRAVh3SToZeHtaPhRU8a
S8EEIcoTVsnBfNfQcADfoe1zvTYfxT+07B9M9Vrrj5sdqpvTtk60I/3nGzEnbA6B
3xbZ+f0fSx9+Q76lhhRlrxNn0TDFWlf2RkCJrCIh5PU+iWi7TnUo3XB7NQIDAQAB
AoGBAIVbS9mXDVfNZydk6LZD+JLQ6czooUOT67vwUXVHbR4pkGyEPvBAdZFpaBRy
aW5gJo0vx4vfOlPqB7fJI/QavBUxzorLK7tYQJJm25E21jyRfacyZ01gf0lVHBkq
sGNu9kM6vodKyc+sXfr6FmC1jmpsGERfdtHV6r1dN4FBUkaBAkEA5mNW1I0dIti6
05h44mDZUomiAiq9clVnsgWdb2fAWZyuDHfvTnWNlVlHsyY+gaH9/vWV+NF9J2an
EB9r+30ysQJBANTnUwjZgGmc/WaUMrCMrjJvyzbz27j0yf7X2IOeU1WUPTewTz+
o8sXpKtlVd4DqxpHg/8dlwWPE1tj/Y3kScUCQHcKp0gGbiKeR05c/0FBd6ldMlfa
S65DUDQ9EH8K5emnuor4wa8RsImV6yVXQn7q+/nsXYSGghuEwBfllH8KztECQQC7
rMrSc0CyWNQ7l4nzfZ+U7tNaTM3XN3ePzepv+shNNziYEsCO7v0d61KaT/LYia1L
th0SRvH3VX8/wa3iZYntAkAo2GS9NUdv9tw/g2eqjqEvZjWMGr8sDxgOPswBiEzP
PjOk2BayboGPY0GNUHXTxn1UMBfoNkzpxXk7KDVFcYF
-----END RSA PRIVATE KEY-----

Private-Key: (1024 bit)
modulus:
00:bf:9a:72:45:8a:a6:db:dc:63:bf:19:7d:e1:28:
97:cb:85:a1:f2:a8:05:b9:c9:10:15:87:74:93:a1:
97:87:b5:a3:e1:45:4f:1a:4b:c1:04:95:ca:2d:56:
c9:c1:7c:db:50:70:00:df:a1:ed:73:bd:36:1f:c5:
3f:b4:ec:1f:4c:f5:5a:eb:8f:9b:1d:aa:9b:d3:b6:
4e:b4:23:fd:e7:1b:31:27:6c:0e:81:df:16:d9:f9:
fd:1f:4b:1f:7e:43:be:88:86:14:65:af:13:67:d1:
30:c5:5a:57:f6:46:40:89:ac:29:61:e4:f5:3e:89:
68:bb:4e:75:28:dd:70:7b:35
publicExponent: 65537 (0x10001)
privateExponent:
00:85:5b:4b:d9:97:0d:57:cd:67:27:64:e8:b6:43:
f8:92:d0:e9:cc:e8:a1:43:93:eb:bb:f0:51:75:47:
6d:1e:29:90:6c:84:3e:f0:40:75:91:69:68:14:72:
69:6e:60:26:8d:2f:c7:8b:df:3a:53:ea:07:b7:c9:
23:f4:1a:bc:15:31:ce:8a:cb:2b:bb:58:40:92:66:
db:91:36:d6:3c:91:7d:a7:32:67:4d:60:7f:49:55:
1c:19:2a:b0:63:6e:f6:43:3a:be:87:4a:c9:cf:ac:
5d:fa:fa:16:60:b5:8e:6a:6c:18:44:5f:76:d1:d5:
ea:bd:5d:37:81:41:52:46:81

prime1:
00:e6:63:56:d4:8d:1d:22:d8:b9:d3:98:78:e2:60:
d9:52:89:a2:02:2a:bd:70:85:67:b2:05:9d:6f:67:
c0:59:9c:ae:0c:77:ef:4e:75:8d:95:59:47:b3:26:
3e:81:a1:fd:fe:f5:95:f8:d1:7d:27:66:a7:10:1f:
6b:fb:7d:32:b1
prime2:
00:d4:e7:53:08:d9:80:69:9c:fd:66:94:32:b0:8c:
ae:32:49:bf:2c:db:cf:6e:e3:d3:2b:7b:5f:62:0e:
79:4d:56:50:f4:de:c1:3c:fe:a3:cb:17:a4:ab:65:
55:de:03:ab:1a:47:83:ff:1d:23:05:8f:13:5b:63:
fd:8d:e4:49:c5
exponent1:
77:0a:a7:48:06:6e:22:9e:47:4e:5c:ff:41:41:77:
a9:5d:32:57:da:4b:ae:43:50:34:3d:10:7f:0a:e5:
e9:a7:ba:8a:f8:c1:af:11:b0:89:95:eb:25:57:42:
7e:ea:fb:f9:ec:5d:84:86:82:1b:84:c0:17:e5:94:
7f:0a:ce:d1
exponent2:
00:bb:ac:ca:d2:73:40:b2:58:d4:3b:97:89:f3:7d:
9f:94:ee:d3:5a:4c:cd:d7:37:77:8f:cd:ea:6f:fa:
c8:4d:37:38:98:12:c0:8e:ee:fd:1d:eb:52:9a:4f:
f2:d8:89:ad:4b:b6:1d:12:46:f1:f7:55:7f:3f:c1:
ad:e2:65:89:ed
coefficient:
28:d8:64:bd:35:47:6f:f6:dc:3f:83:67:aa:8e:a1:
2f:66:35:8c:1a:bf:2c:0f:18:0e:3e:cc:01:88:4c:
cf:3e:33:88:b3:60:5a:c9:b6:86:3d:8d:06:35:41:
d7:4f:19:f5:50:c0:5f:a0:d9:33:a7:15:e4:ec:a0:
d5:15:c6:05

b. Berikut Adalah hasil dari SSL *Certificate Signing Request*, yang telah di *generate*.

SSL Certificate Signing Request
Certificate Signing Request generated!

Generated Certificate Signing Request

-----BEGIN CERTIFICATE REQUEST-----
MIIB9zCCAWACAQAwgZwxCzAJBgNVBAYTAklEMRIwEAYDVQQIEwlJTkRPTkVTSUEx
FDASBgNVBAcTC0RLSSBKQUtBUlRBMRIwEAYDVQQKEwlLT01JU0ktTUkxEDAOBgNV
BAsTB0lUIERFUFQxFjAUBgNVBAMTDWtvbWlzaS1taS5jb20xJTAjBgkqhkiG9w0B
CQEWFmtvbWlzaW1pQGtvbWlzaS1taS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMG9y63/TKM+ftWEnqWVk4L/QUnB55HEM9qXy7j2ski4LfjyFH3pm3Xb
0LQiDLjOt8Qb1IHb+/INrAi5kNDn6pFIdpTEVdVlB06Zqh3XDZ6XkxOeeAi6ukdA
QtDRZEkR9EdqmvjRIh9NPqMq2Ua/W7FoW5ygimzNkzT9ukg0XPE5AgMBAAGgGjAY
BgkqhkiG9w0BCQIxCxMJS09NSVNJLU1JMA0GCSqGSIb3DQEBBAUAA4GBAFay7E58
JocCyTEA+3i6BFMddOCqnlSmxAZ421mMLj4mYTBfl0ktgmlBo8sO2uy2cEjSQQWB
Mi85trfkFb0hMIlUVT9+ytbAmOfZEZutWVi09l84BMlBKSqZwFYeJf50QSD56EW
NeoQMTmwRZzH+mNkp5Cac6FCIL0Fiysa0Yi0
-----END CERTIFICATE REQUEST-----

Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=ID, ST=INDONESIA, L=DKI JAKARTA, O=KOMISI-MI, OU=IT DEPT, CN=komisi-mi.com/emailAddress=komisimi@komisi-mi.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c1:bd:cb:ad:ff:4c:a3:3e:7e:d5:84:9e:a5:95:
93:82:ff:41:49:c1:e7:91:c4:33:da:97:cb:b8:f6:
b2:48:b8:2d:f8:f2:14:7d:e9:9b:75:db:d0:b4:22:
0c:b8:ce:b7:c4:1b:d4:81:db:fb:f9:4d:ac:08:b9:
90:d0:e7:ea:91:48:76:94:c4:55:d5:65:f3:4e:99:
aa:1d:d7:0d:9e:97:93:13:9e:78:08:ba:ba:47:40:
42:d0:d1:64:49:11:f4:47:6a:9a:e8:d1:22:1f:4d:
3e:a3:2a:d9:46:bf:5b:b1:68:5b:9c:a0:8a:6c:cd:
93:34:fd:ba:48:34:5c:f1:39
Exponent: 65537 (0x10001)
Attributes:
unstructuredName :KOMISI-MI
Signature Algorithm: md5WithRSAEncryption
56:b2:ec:4e:7c:26:87:02:c9:31:00:fb:78:b9:04:53:1d:74:
e0:aa:9c:84:a6:c4:06:78:db:59:8c:2e:3e:26:61:30:5f:23:
49:2d:82:69:41:a3:cb:0e:da:ec:b6:70:48:d2:41:05:81:32:
2f:39:b6:b7:e4:15:bd:21:30:89:54:55:3f:7e:ca:d6:c0:98:
e7:d9:11:9b:ad:59:58:b4:f6:5f:38:04:c2:3c:29:2a:99:c0:
56:1e:25:fe:74:42:54:83:e7:a1:16:35:ea:10:31:39:b0:45:
9c:c7:fa:63:64:a7:90:9a:73:a1:42:20:bd:05:8b:2b:1a:d1:
88:b4

c. Berikut Adalah hasil *generate Certificate* (CRT):

SSL Certificate Generated Certificate
SSL Certificate
Generated Certificate

-----BEGIN CERTIFICATE-----
MIIDmDCCAwGgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBlTELMAkGA1UEBhMCNjlx
EjAQBgNVBAgTCUluZG9uZXNpYTEUMBIGA1UEBxMLREtlJIEpha2FydGExDDAKBgNV
BAoTA0JTSTESMBAGA1UECxMJS29taXNpLU1JMRYwFAYDVQQDEw1rb21pc2ktbWku
Y29tMSIwIAYJKoZIhvcNAQkBFhNmcmlleWFkaWVAeWFob28uY29tMB4XDTA1MDgx
NTA0MTMxMloXDTA2MDgxNTA0MTMxMlowgZUxCzAJBgNVBAYTAjYyMRIwEAYDVQQI
EwlJbmRvbmVzaWExFDASBgNVBAcTC0RLSSBKYWthcnRhMQwwCgYDVQQKEwNCU0kx
EjAQBgNVBAsTCUtvbWlzaS1NSTEWMBQGA1UEAxMNa29taXNpLW1pLmNvbTEiMCAG
CSqGSIb3DQEJARYTZnJpZXlhZGllQHlhaG9vLmNvbTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAwlcS9ckg/KnXND18wnAgwDO2ITVDTwHv8Om359UCVWMnbHGt
qHvFr0EwEUDMK/s1yzNrOJgRNPdYQqNiKryMQnf3Uhq9G2z4mviCZGW0ggUqGtC7
2icrF/aR0G/aV8ZftYBTvkI9MeFz5mdHC1e2dDmd9Wqv5NzQE60XUQmjOkCAwEA
AaOB9TCB8jAdBgNVHQ4EFgQUJOQCEYNeV0vqMJPTZ7LuVslg3FcwgcIGA1UdIwSB
ujCBt4AUJOQCEYNeV0vqMJPTZ7LuVslg3FehgZukgZgwgZUxCzAJBgNVBAYTAjYy
MRIwEAYDVQQIEwlJbmRvbmVzaWExFDASBgNVBAcTC0RLSSBKYWthcnRhMQwwCgYD
VQQKEwNCU0kxEjAQBgNVBAsTCUtvbWlzaS1NSTEWMBQGA1UEAxMNa29taXNpLW1p
LmNvbTEiMCAGCSqGSIb3DQEJARYTZnJpZXlhZGllQHlhaG9vLmNvbYIBADAMBgNV
HRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAB6z4BjJ0CqWr5M91XZSSFvfVHIb
erQpyImXyJZx/oM7TNKmZz1FS2BatEKKBbQCr2PPk6iR/HetlEyFA1xt02eptEYx
TzEkhNTpd/cl+kVE3Oj0e5YYNlQB+rAqyo4+zZ9+WYF2R05ZpIpY8pl5PYs4el2v
6YQqGt3BKB3OKsUp
-----END CERTIFICATE-----

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=62, ST=Indonesia, L=DKI Jakarta, O=BSI, OU=Komisi-MI, CN=komisi-mi.com/emailAddress=frieyadie@yahoo.com
Validity
Not Before: Aug 15 04:13:12 2005 GMT
Not After : Aug 15 04:13:12 2006 GMT
Subject: C=62, ST=Indonesia, L=DKI Jakarta, O=BSI, OU=Komisi-MI, CN=komisi-mi.com/emailAddress=frieyadie@yahoo.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c0:87:12:f5:c9:20:fc:a9:d7:34:3d:7c:c2:70:
20:c0:33:b6:b5:35:43:4f:01:ef:f0:e9:b7:e7:d5:
02:55:63:27:6c:71:ad:a8:7b:c5:af:41:30:11:40:
cc:2b:fb:35:cb:33:6b:38:98:11:34:f7:58:42:a3:
62:2a:bc:8c:42:77:f7:52:1a:bd:1b:6c:f8:9a:f8:
82:64:65:b4:82:05:2a:1a:d0:bb:da:27:2b:17:f6:
91:d0:6f:da:57:c6:5f:b5:80:53:be:42:22:f4:c7:
85:cf:99:9d:1c:2d:5e:d9:d0:e6:77:d5:aa:bf:93:
73:40:4e:b4:5d:44:26:8c:e9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
24:E4:02:11:83:5E:57:4B:EA:30:93:D3:67:B2:EE:56:C9:60:DC:57
X509v3 Authority Key Identifier:
keyid:24:E4:02:11:83:5E:57:4B:EA:30:93:D3:67:B2:EE:56:C9:60:DC:57
DirName:/C=62/ST=Indonesia/L=DKIJakarta/O=BSI/OU=Komisi-MI/CN=komisi-mi.com/emailAddress=frieyadie@yahoo.com
serial:00
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: md5WithRSAEncryption
1e:b3:e0:18:c9:d0:2a:96:af:93:3d:d5:76:52:48:5b:df:54:
72:1b:7a:b4:29:c8:89:97:c8:96:71:fe:83:3b:4c:d2:a6:67:
3d:45:4b:60:5a:b4:42:8a:05:b4:02:af:63:cf:93:c8:91:fc:
77:ad:b4:4c:85:03:5c:6d:d3:67:a9:b4:46:31:4f:31:24:84:
d4:e9:77:f7:25:fa:45:44:dc:e8:f4:7b:96:18:36:54:01:fa:
b0:2a:ca:8e:3e:cd:9f:7e:59:81:76:47:4e:59:a5:9a:58:f2:
99:79:3d:8b:38:78:8d:af:e9:84:2a:1a:dd:c1:28:1d:ce:2a:
c5:29

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=62, ST=Indonesia, L=DKI Jakarta, O=BSI, OU=Komisi-MI, CN=komisi-mi.com/emailAddress=frieyadie@yahoo.com
Validity
Not Before: Aug 15 04:13:12 2005 GMT
Not After : Aug 15 04:13:12 2006 GMT
Subject: C=62, ST=Indonesia, L=DKI Jakarta, O=BSI, OU=Komisi-MI, CN=komisi-mi.com/emailAddress=frieyadie@yahoo.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c0:87:12:f5:c9:20:fc:a9:d7:34:3d:7c:c2:70:
20:c0:33:b6:b5:35:43:4f:01:ef:f0:e9:b7:e7:d5:
02:55:63:27:6c:71:ad:a8:7b:c5:af:41:30:11:40:
cc:2b:fb:35:cb:33:6b:38:98:11:34:f7:58:42:a3:

62:2a:bc:8c:42:77:f7:52:1a:bd:1b:6c:f8:9a:f8:
82:64:65:b4:82:05:2a:1a:d0:bb:da:27:2b:17:f6:
91:d0:6f:da:57:c6:5f:b5:80:53:be:42:22:f4:c7:
85:cf:99:9d:1c:2d:5e:d9:d0:e6:77:d5:aa:bf:93:
73:40:4e:b4:5d:44:26:8c:e9

Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
24:E4:02:11:83:5E:57:4B:EA:30:93:D3:67:B2:EE:56:C9:60:DC:57
X509v3 Authority Key Identifier:
keyid:24:E4:02:11:83:5E:57:4B:EA:30:93:D3:67:B2:EE:56:C9:60:DC:57
DirName:/C=62/ST=Indonesia/L=DKI Jakarta/O=BSI/OU=Komisi-MI/CN=komisi-mi.com/emailAddress=frieyadie@yahoo.com
serial:00
X509v3 Basic Constraints:
CA:TRUE

Signature Algorithm: md5WithRSAEncryption
1e:b3:e0:18:c9:d0:2a:96:af:93:3d:d5:76:52:48:5b:df:54:
72:1b:7a:b4:29:c8:89:97:c8:96:71:fe:83:3b:4c:d2:a6:67:
3d:45:4b:60:5a:b4:42:8a:05:b4:02:af:63:cf:93:c8:91:fc:
77:ad:b4:4c:85:03:5c:6d:d3:67:a9:b4:46:31:4f:31:24:84:
d4:e9:77:f7:25:fa:45:44:dc:e8:f4:7b:96:18:36:54:01:fa:
b0:2a:ca:8e:3e:cd:9f:7e:59:81:76:47:4e:59:a5:9a:58:f2:
99:79:3d:8b:38:78:8d:af:e9:84:2a:1a:dd:c1:28:1d:ce:2a:
c5:29

III KESIMPULAN

Dengan adanya beberapa metode di atas, maka untuk keamanan didalam bertransaksi didunia *internet* bisa diatasi kenyamanan dan keamanannya. Biasanya pada saat dilapangan atau pada saat diterapkan kadang terdapat faktor-faktor manusia yang menjadi metode tersebut gagal, diantaranya kelalaian yang menjadi faktor penyebabnya, walaupun masih terdapat beberapa kekurangan-kekurangan pada metode tersebut, akan tetapi sudah bisa diminimalisir terjadinya pembajakan dan kejahatan yang mungkin terjadi.

DAFTAR PUSTAKA

Anoname. 2004. Konsep *Ecommerce*. http://www.sentralweb.com/sentralweb/mod.php?mod=publisher&op=viewarticle&artid=13

Barakatullah, Abdul Halim dan Teguh Prasetyo. 2005. Bisnis *E-Commerce* Studi Sistem Keamanan dan Hukum Di Indonesia. Pustaka Pelajar. Yogyakarta.

Cpanel. 2004. *SSL Manager*. http://www.komisi-mi.com

Eko Indrajit, Richardus Dr, .2005. E-Commerce : Kiat dan Strategi Bisnis Didunia Maya.

Purbo, Onno W. 2000. Mengenal *E-Commerce*. PT. Elex Media Komputindo. Jakarta.

Safitri, Indra. 1999. *E-Commerce* Dalam Persfektif Hukum, http://business.fortunecity.com/buffett/842/art080399_ecommerce.htm

Wikipedia. 2006. Digital Signature. http://en.wikipedia.org/wiki/Digital signature.

_____. 2006. Digital Sertificate. http://en.wikipedia.org/wiki/Digital sertificate

_____. 2006. Transport Layer Security. http://en.wikipedia.org/wiki/TranportLayerSecurity