KONSEP KEAMANAN DALAM E-BUSINESS

Secure Socket Layer (SSL)

SSL (*Secure Socket Layer*) merupakan model pengaman aplikasi-aplikasi berbasis web/internet yang paling banyak digunakan pada saat ini, yakni mengamankan protokol-protokol yang awalnya tidak aman (*insecure*) menjadi aman (*secure*). SSL menjadi mediator antara *user* dengan suatu aplikasi di jaringan Internet yang menggunakan protokol HTTP (*Hyper Text Transfer Protocol*), dengan menampilkan HTTPS (*Hyper Text Transfer Protocol on Secure Socket Layer)* kepada *user*. Pengamanan tersebut dapat juga dilakukan pada protokol-protokol lainnya yang *insecure* seperti POP3 (*Post Office Protocol 3*), SMTP (*Simple Mail Transfer Protocol*), IMAP), IMAP (*Internet Message Access Protocol*) dan lainnya yang merupakan aplikasi pada platform TCP (*Transfer Control Protocol*).

SSL (*Secure Socket Layer*) dikembangkan pertama kali pada awal tahun 1990-an oleh Netscape yang kemudian distandarisasikan oleh International Telecommunication Union (ITU) dan diadopsi oleh Internet Engineering Task Force (IETF), dan dikembangkan lagi menjadi TLS (*Transport Layer Security*) pada akhir 1990-an. SSL awal merupakan SSL versi 3.0, sedangkan TLS dapat dinyatakan sebagai SSL versi 3.1 atau SSH (*Secure Shell*) versi Microsoft.

SSL pada saat dioperasikan, memberikan tahap otentikasi dan pertukaran kunci (*handshake*) dan enkripsi (*encryption*). SSL mengubah protokol HTTP pada port 80 menjadi HTTPS dengan port 443. SSL dapat berjalan bilamana ada suatu aplikasi dalam protokol HTTPS dijalankan. Dengan kata lain, SSL dapat berfungsi jika terjadi suatu *traffic* atau lintas komunikasi data antara *client* dan *server* dengan membentuk suatu *channel*.

Protokol SSL pada dasarnya merupakan sebuah protokol keamanan yang dibentuk antara Application Layer dan Transport Layer pada ruang lingkup TCP/IP (*Transfer Control Protocol/Internet Protocol*). SSL bekerja dengan mengenkripsi dan mendekripsi lalu lintas komunikasi data (*traffic*) dari sebuah atau beberapa aplikasi pada saat terjadi koneksi langsung di Internet. SSL menyediakan layanan-layanan keamanan berikut :

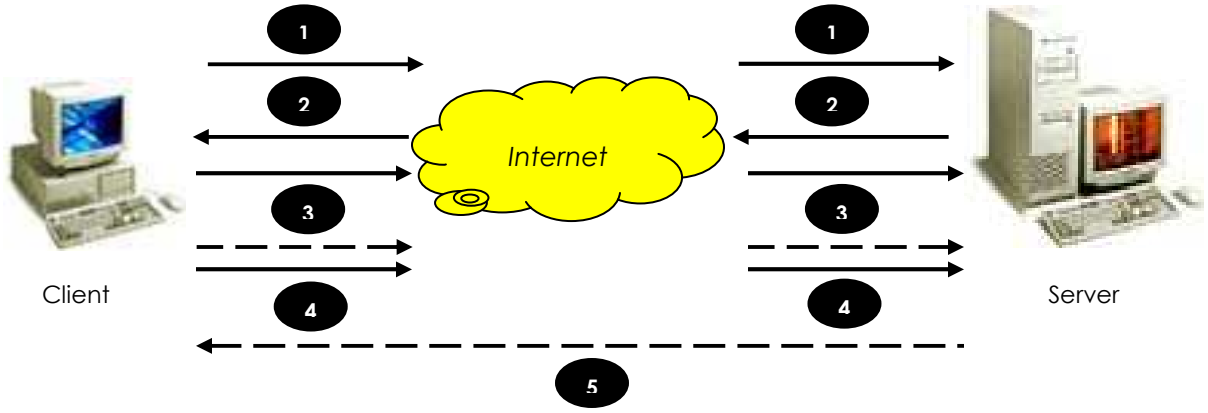
- ***Server Authentication and Client Authentication***, aplikasi-aplikasi dengan SSL dapat menggunakan *Server* atau *Client Certificates* berbasis X.509 untuk mengidentifikasi keaslian Server ataupun Client
- ***Data Confidentiality and Integrity Services***, SSL menyediakan layanan pengenkripsian saluran (*tunnel*) sehingga terbentuk suatu saluran yang aman (*secure tunnel*)

Berikut gambar posisi protokol SSL dalam konsep OSI (*Open Systems Interconnection*) :

Application Layer (SMTP; HTTP)
Presentation Layer
Session Layer (**SSL**)
Transport Layer (TCP/UDP)
Network Layer (IP)

Dengan demikian dapat dinyatakan bahwa SSL menyediakan layanan Authentication, Confidentiality, Integrity seperti pada protokol-protokol di level Application Layer seperti : HTTP, untuk komunikasi web aman; SMTP, untuk transfer email yang aman dan sebagainya.

Protokol SSL/TLS dibangun diatas protokol berbasis Kriptografi Simetris dan Asimetris serta pemanfaatan sertifikasi X.509 (*Simetris* : Transposisi & Substitusi; *Asimetris* : Faktorisasi & Algoritma Diskrit; *Hashing* : Tanda Tangan Digital (Sidik Jari Digital). Selain itu, SSL juga merupakan protokol *'handshake'* berbasis Client-Server yang diimplementasikan seperti yang terlihat pada gambar berikut :



Keterangan :

No. 1 : Client membentuk koneksi awal ke Server dan *request* koneksi SSL

No. 2 : Server dikonfigurasi dan kemudian memberikan *reply* kepada Client berupa pengiriman *Public Key*

No. 3 : Client melakukan otentikasi *Public Key* kepada basis data suatu *Trusted Authorities*. Selanjutnya setelah teridentifikasi bahwa *Public Key* beserta Sertfikatnya terdaftar, dilanjutkan langkah No. 4 (bilamana belum terdaftar, *user* diharuskan mengirimkan Sertfikat dan *Public Key*-nya kepada *Trusted Authorities* tersebut)

No. 4 : Client menggunakan *Public Key* tersebut untuk mengenkripsi suatu *session* Dan kemudian mengirimkan kembali hasilnya berupa *session key* ke Server. (jikalau Server membutuhkan Sertifikat Client pada langkah No. 2, maka Client harus mengirimnya pada langkah ini)

No. 5 : Kalau Server di-setup untuk menerima Sertifikat, maka otomatis Server akan langsung membandingkannya dengan basis data pada *Trusted Authorities* dan selanjutnya akan mengirimkan *reply* apakah menerima atau menolak koneksi yang diminta Client.

Apabila koneksi ditolak, suatu *message* "**gagal**" akan diberikan kepada Client, sedangkan bila diterima Server lalu akan men-decode *session key* (mendekripsi) yang didapat dari Client dengan Private Key milik Server dan mengirimkan *message* "**berhasil**" . Pada proses inilah suatu saluran aman (*Secure Channel*) terbentuk.

.....(Lihat juga gambar Solusi Kriptografi Hybrid SSL/TLS dan Solusi Kriptografi Hybrid S/MIME).....

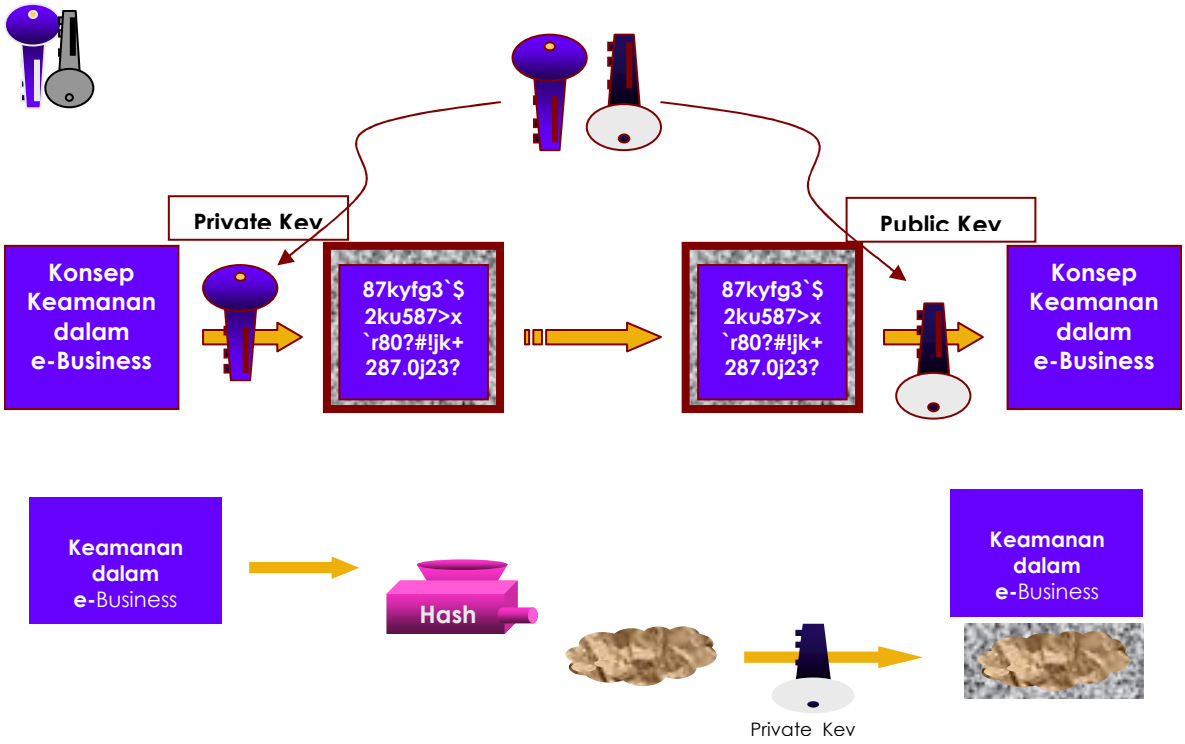
Konsep Sertifikat dan Infrastruktur Kunci Publik (*Public Key Infrastructure*)[1]

Untuk dapat menggunakan blok Kriptografi dalam aplikasi keamanan seperti pada protokol-protokol SSL/TLS, dituntut adanya sebuah infrastruktur keamanan pendukung (*supporting security infrastructures*).

[1] Adopted from *Understanding and Leveraging SSL-TLS for Secure Communication*, Jan De Clercq, Thawte-WindowsIT Pro eBooks, 2005 ch. 1

Sertifikat

Sertifikat adalah sebuah dokumen digital yang membentuk kepercayaan atas kepemilikan sebuah Kunci Publik (*Public Key*). Dalam makna yang lebih sempit, Sertifikat menyediakan sebuah '*tool*' untuk mem-verifikasi klaim bahwa sebuah Kunci Publik dimiliki oleh sebuah entitas spesifik. Untuk itu sebuah Tanda Tangan Digital perlu ditambahkan ke dalam Sertifikat. Pihak penerbit Sertifikat (*Certificate Authority : CA*), menerapkan Tanda Tangan Digital dengan menggunakan sebuah Kunci Privat (*Private Key*). Model pembuatan Tanda Tangan Digital adalah dengan menggunakan algoritma SHA1, SHA2 (*Secure HashAlgorithm1-2*) dan MD5 (*Message Digest5*) seperti diilustrasikan berikut :



Infrastruktur Kunci Publik (IKP)

IKP yang distandarisasikan oleh IETF (*Internet Engineering Task Force*) menyediakan sebuah rangkaian blok pengaman lewat layanan-layanan, kebijakan dan prosedur keamanan bagi para penggunanya yang mencakup verifikasi dan otentikasi validitas setiap transaksi yang melalui jaringan. Dalam ruang lingkup e-business, kemajuan pengamanan transaksi tergantung pada jenis IKP yang diimplementasikan. Diantara blok pengaman yang dapat ditawarkan oleh IKP adalah sebagai berikut :

1. *Identification*, memberikan entitas sebuah cara untuk mengecek identitas entitas lainnya.
2. *Data Authentication*, menyediakan cara untuk menjamin bahwa pengirim/penerima pesan adalah pihak yang sah/berhak.
3. *Confidentiality*, sebuah layanan yang melindungi terhadap dibukanya informasi tanpa wewenang pihak yang berhak.
4. *Integrity*, sebuah layanan keamanan yang melindungi terhadap modifikasi pesan yang tidak terdeteksi.
5. *Non-Repudiation*, melindungi terhadap pengingkaran oleh salah satu entitas yang terlibat dalam sebuah komunikasi.

Dapat dinyatakan pula bahwa IKP merupakan implementasi Kriptografi Asimetris yang memanfaatkan penggunaan Kunci Publik (*Public Key*) dan Kunci Privat (*Private Key*). IKP juga menyediakan layanan untuk mengelola kunci-kunci tersebut beserta siklus hidupnya secara menyeluruh (*Certificates Collecting and Management*) seperti : Sertifikasi, Registrasi User, Pertukaran Kunci (*Key Exchange*), Penerbitan Sertifikat, Pembaharuan Sertfikat, Penyimpanan Sertifikat dan lainnya.

Virtual Private Network (VPN)

Saat ini dibeberapa negara, VPN dijadikan model pengaman jaringan transaksi e-business. VPN beroperasi dengan mensimulasikan sebuah jaringan privat diatas jaringan publik (*internet*) dengan mengenkripsi komunikasi diantara dua "*end-points*" secara privat. Perangkat-perangkat VPN dapat digunakan untuk menciptakan sebuah '*tunnel*' non-aplikasi yang terenkripsi secara semi-permanen diantara dua komputer '*host*' yang mengijinkan jaringan komputer-komputer tersebut untuk melakukan pertukaran di dalam cakupan berbagai aplikasi atau protokol (tidak semata hanya pada pertukaran suatu aplikasi berbasis aplikasi).

Awalnya, metode untuk mengamankan sebuah '*tunnel*' dalam jaringan komputer global berbasis VPN adalah dengan menggunakan protokol Internet Protocol Security (*IPSec*) (merupakan protokol standar untuk membangun VPN). IPSec membutuhkan biaya infrastruktur yang lebih besar, kompleks dan sangat kuat dalam mengamankan komunikasi data, seperti dengan adanya implementasi *Internet Key Exchange* (IKE); sebuah protokol "*handshake*".

VPN memungkinkan 'private intranet' dikembangkan secara aman melalui enkripsi IPSec di jaringan Internet atau layanan jaringan lain, menyediakan keamanan dalam bertransaksi e-commerce, dan koneksi extranet dengan karyawan yang berpindah-pindah lokasi tugas, mitra bisnis, pemasok, pelanggan dan lainnya. VPN memberikan manfaat antara lain efisiensi biaya, keamanan dan kecepatan akses, simplifikasi topologi jaringan; baik secara internal, maupun dengan pihak eksternal seprti pemasok, mitra bisnis dan sebagainya.

Ada tiga tipe utama VPN yakni[2] :

1. **Remote Access VPN**
   Koneksi *user-to-LAN* (*corporate LAN*) secara *remote* dari lokasi *user* berada. Biasanya diaplikasikan oleh *individual dial-up user*.
2. **Site-to-Site VPN**
   Koneksi antara gedung atau lokasi kerja (*branch office*) dan kantor pusat (*main office, headquarters*) dengan membentuk global intranet.
3. **Extranet VPN**
   Koneksi dengan mitra bisnis, pemasok, pelanggan untuk tujuan e-commerce yang aman (menghubungkan dua entitas/perusahaan secara aman). Merupakan ekstensi dari Intranet VPN dengan menambahkan Firewall sebagai proteksi internal.

Kini dimunculkan metode pengaman pertukaran informasi dan transaksi bisnis dengan mengimplementasikan VPN berbasis protokol SSL/TLS (*SSL based-VPN*) yang lebih sederhana dan mudah digunakan dibandingkan VPN berbasis IPSec.

[2] Adopted from *Network Security First-Step*, Tom Thomas, 1st edition, Pearson Education, Inc., 2004 p. 272-282