VOL. II. NO. 1. MARET 2001 ISSN:1411-3201

JURNAL ILMIAH DASI

DATA EKONOMI, BISNIS DAN TEKNOLOGI INFORMASI

AKADEMI MANAJEMEN INFORMATIKA DAN KOMPUTER
"AMIKOM" YOGYAKARTA

DIGITAL SIGNATURE DALAM ELECTRONIC COMMERCE

Sudarmawan

PENDAHULUAN

Perniagaan Elektronik yang sering kita sebut dengan *Electronic Commerce*, sebagai bagian dari bisnis yang dilakukan dengan menggunakan *electronic transmission* (*Electronic Business*), oleh para ahli dan pelaku bisnis dicoba dirumuskan definisinya dari terminologi E-Commerce (Perniagaan Elektronik). Secara umum e-commerce dapat didefinisikan sebagai segala bentuk transaksi perdagangan/perniagaan barang atau jasa (*trade of goods and service*) dengan menggunakan media elektronik. Jelas, selain dari yang telah disebutkan di atas, bahwa kegiatan perniagaan tersebut merupakan bagian dari kegiatan bisnis.

Saat ini jaringan internet merupakan media yang banyak digunakan untuk penyelenggaraan E-Commerce, mengingat penggunaan media internet yang saat ini paling populer digunakan oleh banyak orang, selain merupakan hal yang bisa dikategorikan sebagai hal yang sedang 'booming'. Perlu digarisbawahi, dengan adanya perkembangan teknologi di masa mendatang, terbuka kemungkinan adanya penggunaan media jaringan lain selain internet dalam e-commerce. Jadi pemikiran kita jangan hanya terpaku pada penggunaan media internet belaka.

Penggunaan internet dipilih oleh kebanyakan orang sekarang ini karena kemudahan-kemudahan yang dimiliki oleh jaringan internet:

1. Internet sebagai jaringan publik yang sangat besar (*huge/widespread network*), layaknya yang dimiliki suatu jaringan publik elektronik, yaitu murah, cepat dan kemudahan akses.
2. Menggunakan electronic data sebagai media penyampaian pesan/data sehingga dapat dilakukan pengiriman dan penerimaan informasi secara mudah, ringkas dan cepat.

Koneksi ke dalam jaringan internet sebagai jaringan publik merupakan koneksi yang tidak aman. Hal ini menimbulkan konsekuensi bahwa E-commerce yang dilakukan dengan koneksi ke internet adalah merupakan bentuk transaksi beresiko tinggi yang dilakukan di media yang tidak aman.

Salah satu cara untuk mengatasi kelemahan yang dimiliki oleh internet sebagai jaringan publik yang tidak aman ini dengan adanya penerapan teknologi penyandian informasi (Crypthography). Electronic data transmission dalam e-commerce akan

dilewatkan suatu algoritma penyandian (proses enkripsi) sehingga menjadi data tersandi (cipher/locked data) yang hanya bisa dibaca/dibuka dengan melakukan proses reversal yaitu proses dekripsi. Pada saat data masih dalam jaringan lokal akan terproteksi oleh firewall yang kita pasang sedangkan pada saat data ditransmisikan melalui jaringan publik dimana data harus melewati beberapa router (point-to-point) data dapat diserang. Langkah penyandian ini dilakukan untuk melindungi data dari serangan pada saat data melewati sebuah router/mesin perantara.

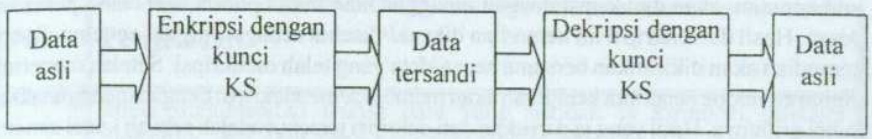
Perlu diperhatikan bahwa, kelemahan hakiki dari open network yang telah dikemukakan tersebut semestinya dapat diantisipasi atau diminimalisasi dengan adanya sistem pengamanan jaringan yang juga menggunakan kriptografi terhadap data dengan menggunakan sistem pengamanan dengan Digital Signature.

DIGITAL SIGNATURE

Tujuan dari suatu tandatangan dalam suatu dokumen adalah untuk memastikan otentisitas dari dokumen tersebut. Suatu digital signature sebenarnya adalah bukan suatu tanda tangan seperti yang kita kenal selama ini, ia menggunakan cara yang berbeda untuk menandai suatu dokumen sehingga dokumen atau data tidak hanya mengidentifikasi dari pengirim, namun ia juga memastikan keutuhan dari dokumen tersebut tidak berubah selama proses transmisi. Suatu digital signature didasarkan dari isi dari pesan itu sendiri.

Digital Signature adalah suatu sistem pengamanan yang menggunakan public key cryptography system. Bedasarkan sejarahnya, penggunaan digital signature berawal dari penggunaan teknik kriptografi yang digunakan untuk mengamankan informasi yang hendak ditransmisikan/disampaikan kepada orang lain yang sudah digunakan sejak ratusan tahun yang lalu. Dalam suatu kriptografi suatu pesan dienkripsi (encrypt) dengan menggunakan suatu kunci (key). Hasil dari enkripsi ini berupa chipertext yang kemudian ditransmisikan/diserahkan kepada tujuan yang dikehendakinya. Chipertext tersebut kemudian dibuka/didekripsi (decrypt) dengan suatu kunci untuk mendapatkan informasi yang telah dienkripsi tersebut. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris (symetric crypthography/secret key crypthography) dan kriptografi asimetris (asymetric crypthography) yang kemudian lebih dikenal sebagai public key crypthography.

Secret key crypthografi atau yang dikenal sebagai kriptografi simetris, menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi terhadap suatu pesan (message), disini pengirim dan penerima menggunakan kunci yang sama sehingga mereka harus menjaga kerahasian (secret) terhadap kuci tersebut. Salah satu algoritma yang terkenal dalam kriptografi simetris ini adalah Data Encryption standard (DES).



Gambar 1 : kriptografi simetris

Public key crypthography, atau dikenal juga sebagai kriptografi asimetris, menggunakan dua kunci (key) : satu kunci digunakan untuk melakukan enkripsi terhadap suatu pesan (messages) dan kunci yang lain digunakan untuk melakukan dekripsi terhadap pesan tersebut. Kedua kunci tersebut mempunyai hubungan secara matematis sehingga suatu pesan yang dienkripsi dengan suatu kunci hanya dapat didekripsi dengan kunci pasangannya. Seorang pengguna mempunyai dua buah kunci, yaitu sebuah kunci privat (privat key) dan juga sebuah kunci publik (public key). Pengguna (user) tersebut kemudian mendistribusikan/menyebarluaskan kunci publik miliknya. Karena terdapat hubungan antara kedua kunci tersebut, pengguna dan seseorang yang menerima kunci publik akan merasa yakin bahwa suatu data yang diterimanya dan telah berhasil didekripsi hanya dapat berasal dari pengguna yang mempunyai kunci privat. Kepastian /keyakinan ini hanya ada selama kunci privat ini tidak diketahui oleh orang lain. Kedua kunci ini berasal atau diciptakan sendiri oleh penggunanya. Salah satu algoritma yang terbaik yang dikenal selama ini adalah RSA (dinamakan sesuai dengan nama penciptanya Rivest, Shamir, Adleman).

Gambar 2 : kriptografi dengan menggunakan kunci publik

Pada saat dua orang hendak saling berkomunikasi atau saling bertukar data/pesan secara aman, mereka kemudian saling mengirimkan salah satu kunci yang dipunyainya, yaitu kunci publiknya. Sedangkan mereka menyimpan kunci prifat sebagai pasangan dari kunci publik yang didistribusikannya. Karena data/pesan ini hanya dapat dienkripsi dan dekripsi dengan menggunakan kunci pasangannya maka data ini dapat dapat ditransmisikan dengan aman melalui jaringan yang relatif tidak aman (melalui internet).

Dalam Digital signature suatu data/pesan akan dienkripsi dengan menggunakan kunci simetris yang diciptakan secara acak (randomly generated symmetric key). Kunci

ini kemudian akan dienkripsi dengan menggunakan kunci publik dari calon penerima pesan. Hasil dari enkripsi ini kemudian dikenal/disebut sebagai "digital envelope" yang kemudian akan dikirimkan bersama pesan/data yang telah dienkripsi. Setelah menerima digital envelope penerima kemudian akan membuka/mendekripsi dengan menggunakkan kunci prifatnya. Hasil yang ia dapatkan dari dekripsi tersebut adalah sebuah kunci simetris yang dapat digunakannya untuk membuka data/pesan tersebut.

Kombinasi antara digital signature dengan message digest menyebabkan seorang pengguna dapat "menandatangani secara digital" (digitally sign) suatu data/pesan. Maksud dari menandatangani secara digital adalah memberikan suatu ciri khas terhadap suatu pesan. Message digest adalah suatu besaran (value) yang berasal dari suatu data/pesan yang memiliki sifat yang unik yang menandai bahwa pesan tersebut mempunyai suatu besaran tertentu. Messages digest diciptakan dengan melakukan enkripsi terhadap suatu data dengan menggunakan kriptografi satu arah (one way crypthography), yaitu suatu teknik kriptografi yang terhadapnya tidak dapat dilakukan proses pembalikan (reversed). Pada saat message digest dienkripsi dengan menggunakan kunci privat dari pengirim dan "ditambahkan" kepada data/pesan yang asli maka hasil yang didapat adalah digital signature dari pesan tersebut.

Penerima dari digital signature akan dapat mempercayai bahwa data/pesan benar berasal dari pengirim. Dan karena apabila terdapat perubahan suatu data/pesan akan menyebabkan akan merubah message digests dengan suatu cara yang tidak dapat diprediksi (in unpredictible way) maka penerima akan merasa yakin bahwa data/pesan tersebut tidak pernah diubah setelah message digest diciptakan.

Sebelum kedua belah pihak (pengirim/penerima) hendak melakukan komunikasi diantaranya dengan menggunakan kriptografi kunci publik, masing-masing pihak harus merasa yakin akan keberadaan mereka. Mereka kemudian akan melakukan otentifikasi terhadap keberadaan masing-masing pihak. Agar mereka dapat melakukan otentifikasi terhadap keberadaan mereka masing-msing maka mereka menunjuk pihak ketiga yang akan memberikan otentifikasi terhadap kunci publik mereka. Pihak ketiga ini kita kenal sebagai Certification Authorithy. Certification authorithy ini kemudian akan memberikan suatu sertifikat (certificate) yang berisi identitas dari pengguna, sertifikat ini ditandatangani secara digital oleh Certification authority tersebut. Isi dari sertifikat tersebut selain identitas ia juga berisi kunci publik dari pemiliknya.

Untuk lebih mudah memahami digital signature berikut ini contoh dari penggunaan digital signature dalam bentuk tabel proses-proses yang terjadi apabila Shela ingin menandatangani suatu pesan dan mengirimkannya kepada Sephia.

No	Penjelasan
1	Shela menjalankan (runs) data yang hendak ia kirimkan, melalui algoritma satu arah (one way algorithm) sehingga ia mendapat suatu nilai (value) yang unik dari data tersebut. Nilai ini disebut message digest. Nilai adalah semacam sidik jari bagi data tersebut dan akan digunakan dalam proses yang lebih lanjut untuk meneliti keutuhan (integrity) dari data tersebut.
2	Shela kemudian melakukan enkripsi terhadap messages digest tersebut dengan menggunakan kunci prifatnya sehingga ia akan mendapatkan digital signature dari data tersebut.
3	Kemudian, Shela membuat (generates) suatu kunci simetris secara acak (random) dan menggunakan kunci itu melakukan enkripsi terhadap data yang hendak ia kirimkan, digital signature miliknya, dan salinan dari sertifikat digitalnya yang berisi kunci publiknya. Untuk mendekripsi data tersebut Sephia membutuhkan salinan dari kunci asimetris tersebut.
4	Shela harus memiliki terlebih dahulu sertifikat milik Sephia, sertifikat ini berisi salinan (copy) dari kunci publik milik Sephia. Untuk menjamin keamanan transmisi dari kunci simetris maka kunci tersebut dienkripsi dengan menggunakan kunci publik milik Sephia. Kunci yang telah dienkripsi yang dikenal sebagai amplop digital (digital envelope) akan dikirimkan bersama-sama dengan data yang telah dienkripsi.
5	Shela kemudian akan mengirimkan data (message) tersebut yang berisi data yang telah dienkripsi dengan kunci simetris, tandatangan dan sertifikat digital, serta kunci simetris yang telah dienkripsi dengan kunci asimetris (digital envelope).
6	Sephia menerima pesan (messages) dari Shela tersebut dan kemudian mendekripsi amplop digital dengan kunci prifat yang dipunyainya, ia kemudian akan mendapatkan kunci simetris.
7	Sephia kemudian menggunakan kunci simetris tersebut untuk mendekripsi data itu (property descryption), tandatangan Shela, dan sertifikat miliknya.
8	Ia kemudian mendekripsi digital signature milik Shela dengan menggunakan kunci publik milik Shela, yang didapat Sephia dari sertifikat milik Shela. Dari dekripsi ini akan didapatkan message digest dari data tersebut.

9	Sephia kemudian memproses (run) data itu dengan menggunakan algoritma satu arah yang sama yang digunakan Shela untuk message digest.
10	Akhirnya Sephia akan membandingkan antara message digest yang didapatkannya dari proses dekripsi diatas dengan message digest yang didapatkan dari digital signature milik Shela. Kalau hasil yang didapat dari perbandingan itu adalah sama maka, Sephia dapat merasa yakin bahwa data tersebut tidak pernah dirusak (altered) selama proses transmisi dan data itu ditandatangani dengan menggunakan kunci privat milik Shela. Kalau hasil dari perbandingan itu adalah tidak sama, maka data tersebut pastilah telah diubah atau dipalsukan setelah ditandatangani.

KESIMPULAN

Suatu tanda tangan digital (Digital Signature) akan menyebabkan data elektronik yang dikirimkan melalui open network tersebut menjadi terjamin dan jaminan keamanan data di E-Commerce merupakan masalah utama. Pentingnya enkripsi baik simetris maupun asimetris perlu kiranya mahasiswa kita (AMIKOM) untuk diperkenalkan dan didorong mempelajari algoritma-algoritma enkripsi dan dekripsi bisa RSA atau DES.

DAFTAR PUSTAKA

1. Andrew S Tanenbaum : *Jaringan Komputer (jilid 2)*, Prenhallindo, Jakarta, 1997
2. Onno W : *Internet dan multimedia* (makalah seminar nasional KMI AMIKOM 30 september 2000)