APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

STRATEGI DAN IMPLEMENTASI E-COMMERCE

Topik Bahasan

IMPLEMENTASI DIGITAL SIGNATURE DALAM PROSES AUTENTIFIKASI

Versi

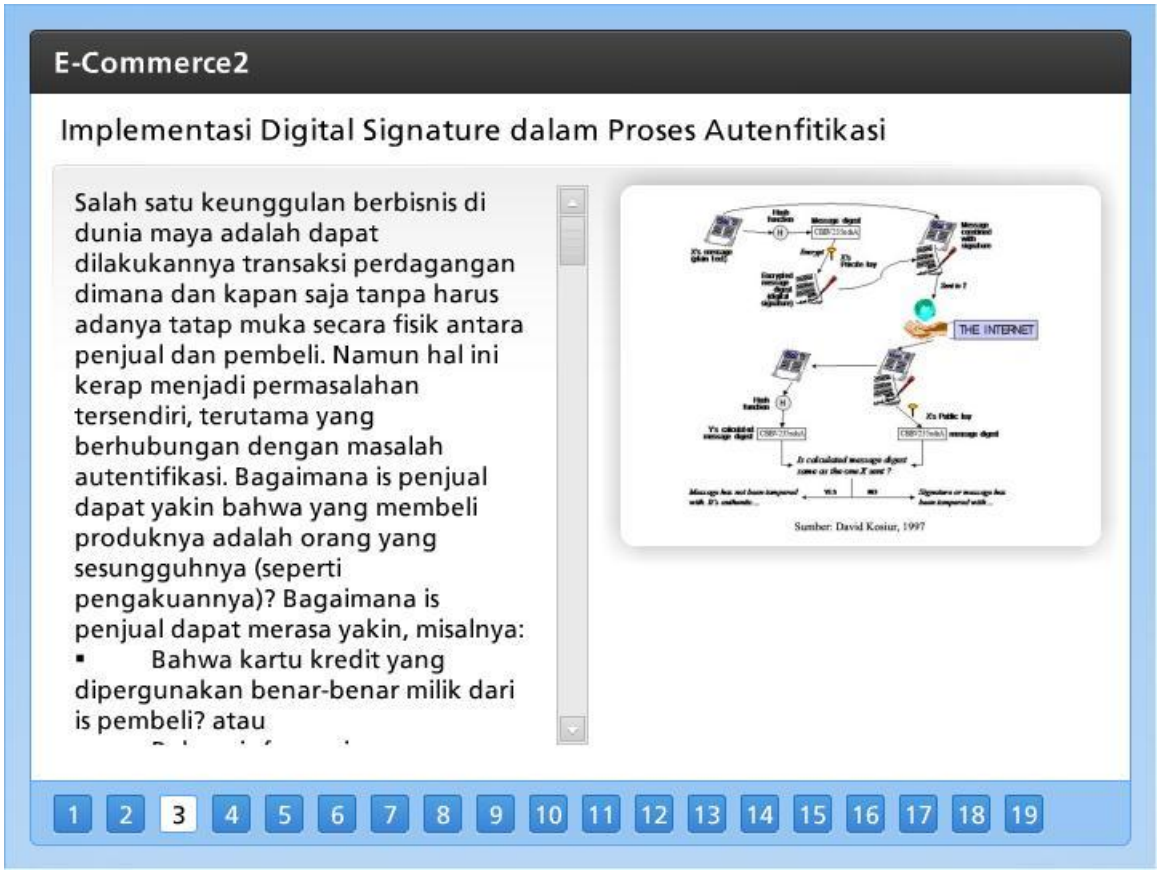
2013/1.0

Nama File

SDIE-8B-ImplementasiDigital.pdf

Referensi Pembelajaran

8-B



Salah satu keunggulan berbisnis di dunia maya adalah dapat dilakukannya transaksi perdagangan dimana dan kapan saja tanpa harus adanya tatap muka secara fisik antara penjual dan pembeli. Namun hal ini kerap menjadi permasalahan tersendiri, terutama yang berhubungan dengan masalah autentifikasi. Bagaimana is penjual dapat yakin bahwa yang membeli produknya adalah orang yang sesungguhnya (seperti pengakuannya)? Bagaimana is penjual dapat merasa yakin, misalnya:

- Bahwa kartu kredit yang dipergunakan benar-benar milik dari is pembeli? atau
- Bahwa informasi yang dikirimkan oleh is penjual tidak jatuh ke tangan mereka yang tidak berhak kecuali pembeli yang bersangkutan? atau
- Bahwa dokumen yang dikirimkan tidak diubah-ubah oleh mereka yang tidak berhak di tengah-tengah jalur transmisi? atau
- Bahwa transaksi perdagangan dapat sah secara hukum karena tidak adanya pihak penipuan dari is pembeli?
- dan lain sebagainya.

Di dalam dunia nyata, biasanya untuk memecahkan permasalahan ini dipergunakan "tanda tangan" sebagai bukti autentifikasi (keaslian) identifikasi seseorang. Di dalam dunia maya, ditawarkan suatu konsep yang diberi nama sebagai "Digital Signature" atau tanda tangan digital (Kosiur, 1997). Prinsip dari implementasi sebuah sistem digital signature adalah seperti yang dijelaskan berikut ini.

Berbeda dengan metoda "public-key encryption" yang secara teknis membutuhkan waktu yang relatif lama untuk melakukan enkripsi (pengkodean acak) terhadap sebuah dokumen, pada sistem digital signature, dokumen yang dikirimkan tidak dienkripsi dengan menggunakan kunci publik (public key).

Sumber: David Kosiur, 1997

Dokumen tersebut dikodekan dengan menggunakan sebuah fungsi matematika yang dinamakan "Hash Function". Dengan menggunakan tipe Hash Function 16 bytes, maka teks yang panjang akan dapat dinyatakan dalam 16 buah karakter, misalnya menjadi: CBBV235ndsAG3D67 yang dinamakan sebagai "message digest". Si pengirim kemudian dengan menggunakan kode pribadinya (private key) melakukan enkripsi terhadap message digest ini, dan hasilnya adalah tanda tangan digital (digital signature) dari si pengirim. Digital signature inilah yang kemudian digabungkan dengan teks yang ada (dokumen asli) untuk kemudian dikirimkan melalui internet.

Di pihak penerima akan diadakan serangkaian proses autentifikasi. Proses pertama adalah memisahkan antara dokumen asli dengan digital signature yang menyertainya. Proses kedua adalah memberlakukan kembali Hash Function terhadap dokumen asli sehingga didapatkan 16 karakter message digest. Proses ketiga adalah melakukan proses dekripsi terhadap digital signature dengan menggunakan kunci public (public key) dari si pengirim. Proses selanjutnya adalah memperbandingkan atau mengkomparasikan 16 karakter message digest hasil Hash Function dan aktivitas dekripsi. Jika kedua message digest tersebut

identik, maka dokumen dan digital signature yang diterima adalah otentik, berasal dari orang yang dimaksud dan tidak diintervensi oleh yang tidak berhak dalam perjalanan transmisinya. Sebaliknya jika ternyata kedua message digest tersebut tidak sama, berarti ada tiga kemungkinan yang terjadi:

- Dokumen yang dikirimkan telah mengalami perubahan dari segi isi;
- Digital Signature yang dikirimkan telah mengalami modifikasi; atau
- Kedua-duanya telah mengalami perubahan sehingga tidak sama dengan aslinya.

Tentu saja perubahan tersebut dapat terjadi karena disengaja maupun tidak. Disengaja dalam arti kata bahwa ada seseorang atau pihak lain yang mencoba untuk mengganti dokumen atau memalsukan digital signature; tidak sengaja dalam arti kata mungkin saja terjadi "kerusakan" teknis, baik secara hardware maupun software, sepanjang media transmisi sehingga terjadi perubahan data yang dikirim. Satu-satunya permasalahan dari metoda autentifikasi ini adalah pengiriman dokumen asli tanpa harus dilakukan proses enkripsi (karena dinilai lambat, terutama jika dokumennya berisi teks yang sangat panjang). Namun konsep "pareto" dapat dipergunakan, dalam arti kata menerapkan asumsi bahwa 80% dari komunikasi adalah "aman". Jika ternyata terjadi "intervensi" pada jalur transmisi, alternatif kedua yaitu penggunaan "symmetric encryption" atau "public-key encryption" dapat dipakai sebagai alternatif.