E-Commerce

Digital Authentification

Teknik Informatika

Preview

- Keunggulan Bisnis di Internet yaitu dapat dilakukannya transaksi perdagangan dimana dan kapan saja tanpa harus adanya tatap muka secara fisik antara penjual dan pembeli.

Preview

Kendala : bagaimana penjual merasa yakin :

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

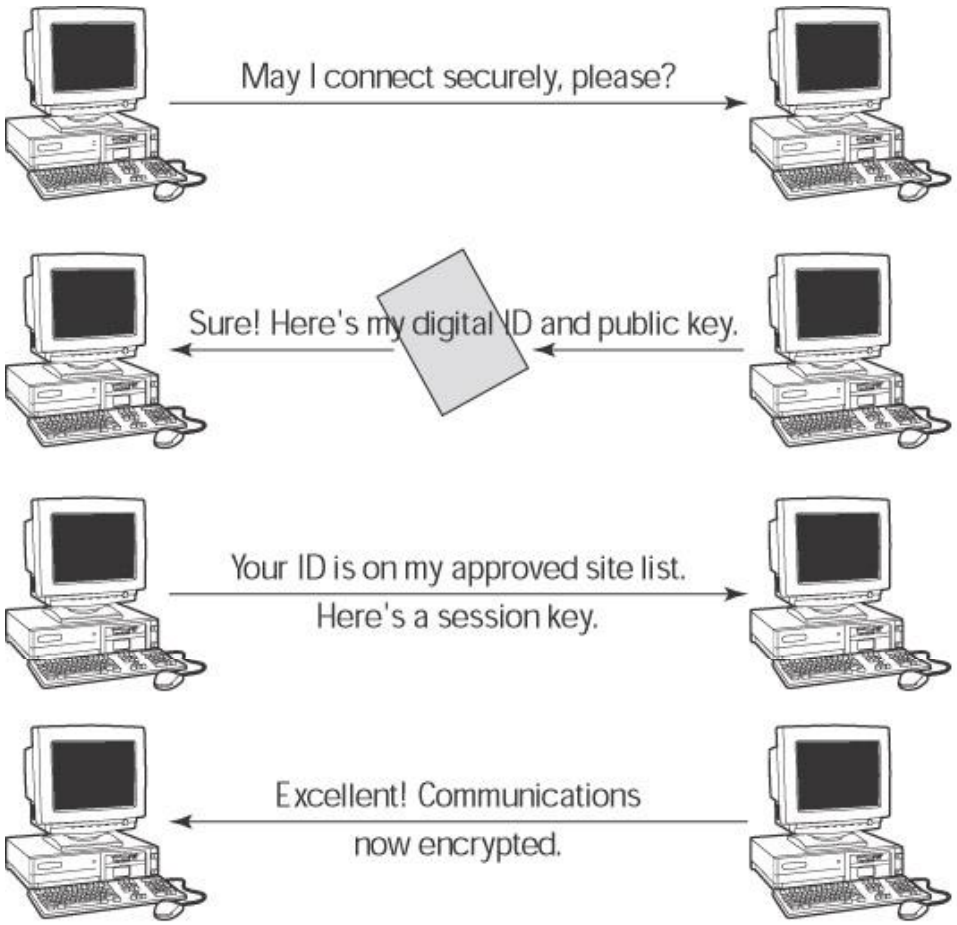
Digital Signature

- 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).

Public Key

- Public key cryptography adalah sebuah skema asimetris dimana menggunakan sepasang kunci untuk enkripsi, yaitu sebuah public key, dimana untuk mengenkripsi data dan dekripsi secara rahasia.
- Anda mem-publis public key anda dan menyimpan private key anda. Seseorang yang memiliki public key dapat mengirimkan sebuah pesan terenkripsi dimana hanya anda yang dapat membacanya.
- Seseorang tersebut hanya dapat mengenkripsi, tetapi tidak dapat mendekripsi.

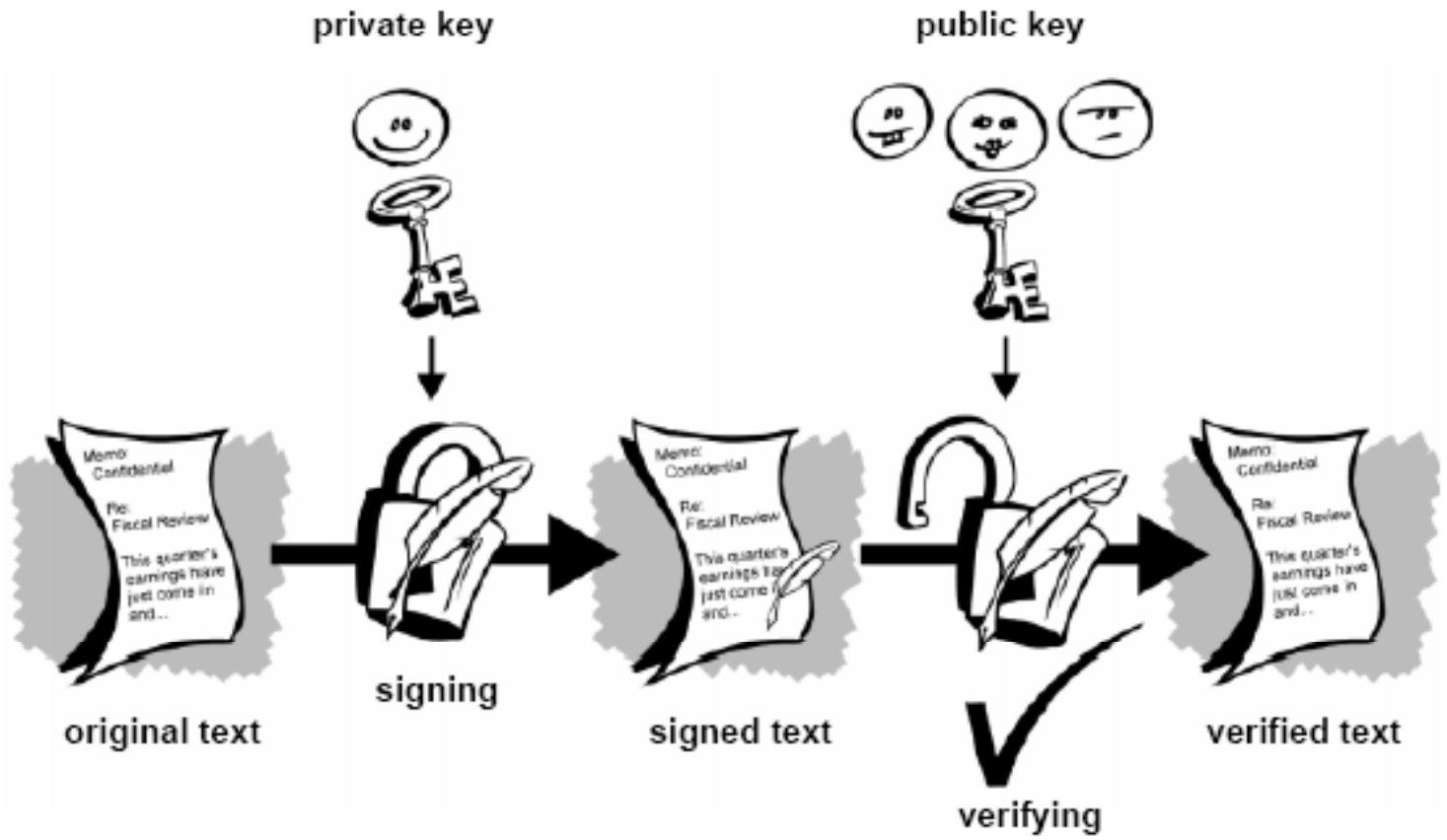
Konsep Digital Signature



Gambar 1. Transaksi e-commerce terenkripsi

Cryptography for Dummies, by Chey Cobb - John Wiley & Sons

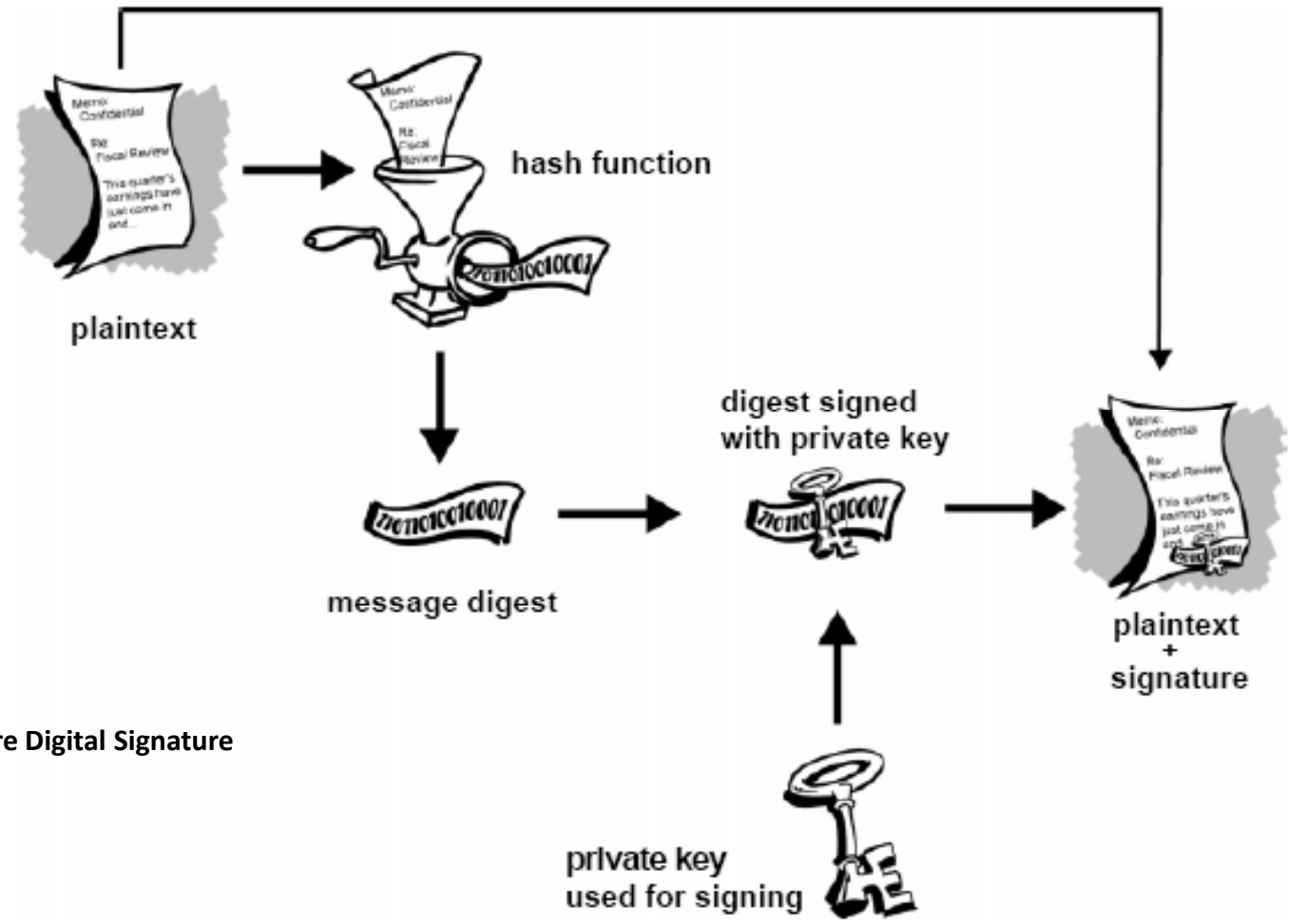
Simple Digital Signature



Gambar 2. Simple Digital Signature

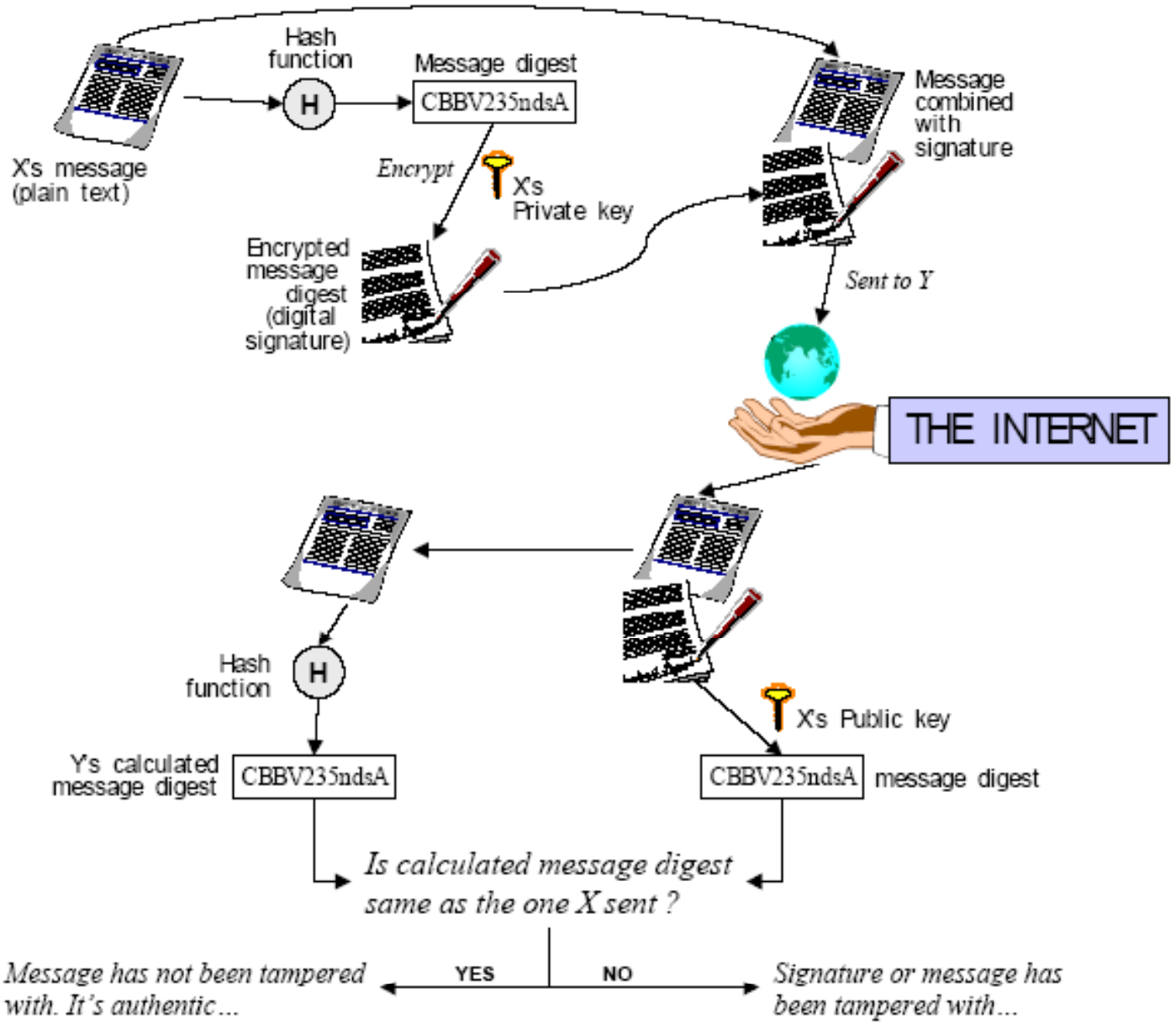
An Introduction to Cryptography, Network Associates, Inc.

Secure Digital Signature



Gambar 3. Secure Digital Signature

An Introduction to Cryptography, Network Associates, Inc.



Sumber: David Kosiur, 1997

Secure Digital Signature – Pengirim (1/2)

1. 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*".

Secure Digital Signature – Pengirim (2/2)

2. 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.
3. Digital signature inilah yang kemudian digabungkan dengan teks yang ada (dokumen asli) untuk kemudian dikirimkan melalui internet.

Secure Digital Signature – Penerima (1/2)

Tahap autentifikasi pada penerima:

1. Memisahkan antara dokumen asli dengan digital signature yang menyertainya.
2. Memberlakukan kembali Hash Function terhadap dokumen asli sehingga didapatkan 16 karakter message digest.
3. Melakukan proses dekripsi terhadap digital signature dengan menggunakan kunci public (public key) dari si pengirim.

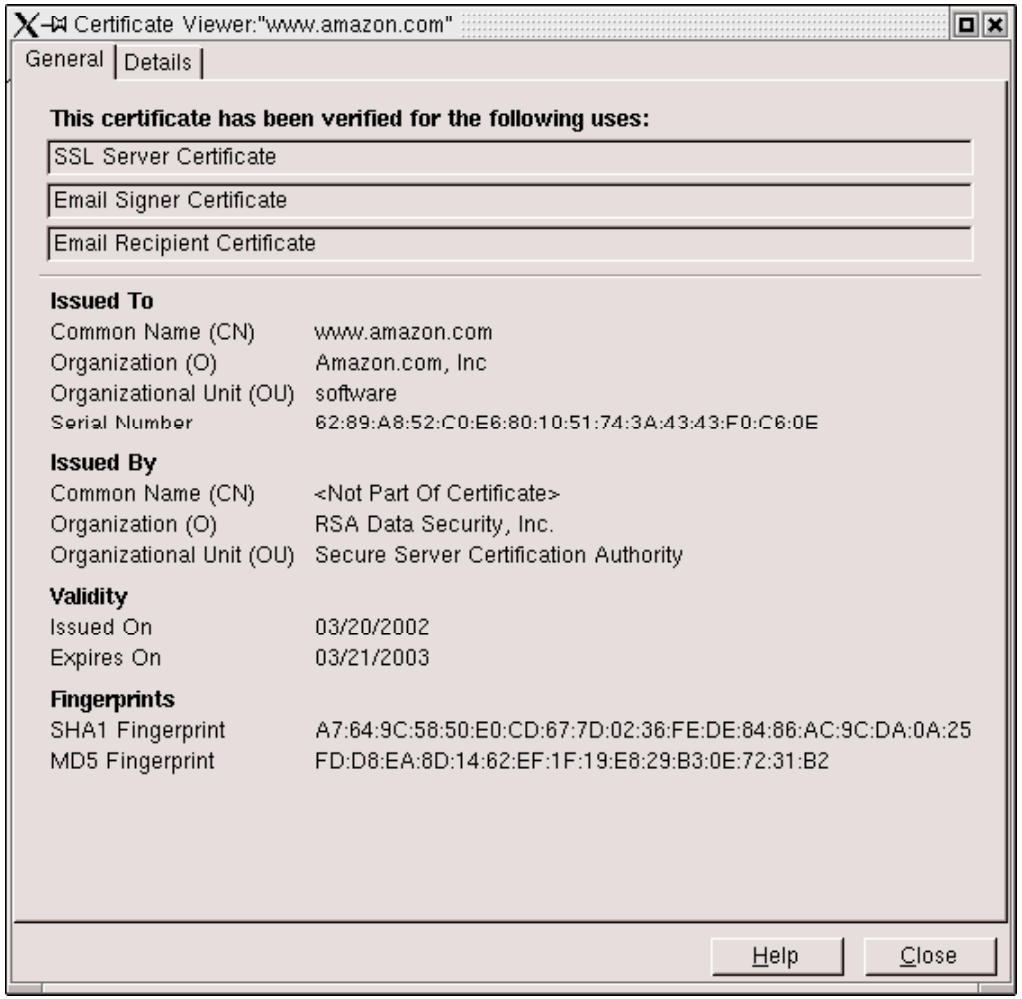
Secure Digital Signature – Penerima (2/2)

4. Memperbandingkan 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.
   - Jika tidak sama, maka kemungkinannya :
     - dokumen ada perubahan,
     - digital signature mengalami modifikasi,
     - dokumen dan digital signature mengalami perubahan, sehingga tidak sama dengan aslinya.

Certificate Authority dan Digital Certificate

- Mempercayakan kepada perusahaan penyedia *digital certificates* untuk membuktikan kebenaran dari layanan transaksi elektronis.
- Digital certificate seperti halnya SIM (Surat Ijin Mengemudi) atau KTP (Kartu Tanda Penduduk).
- Digital certificate dapat membantu seseorang menentukan keaslian dari sebuah layanan
  - Public key
  - Subjek, Penerbit, Diterbitkan untuk, Periode validitas, …
  - Satu atau lebih digital signature

Certificate Authority dan Digital Certificate



Certificate Authority dan Digital Certificate

- Layanan dari Certificate Authority
  - Memverifikasi request sebuah digital certificate
  - Membuktikan request dan menerbitkan digital certificate
  - Memanage digital certificate yang diterbitkan
    - Validitas
    - Perpanjangan
    - Pemeliharaan dari Certificate Revocation List (CRL)
- Model kepercayaan (*Model of trust*)
  - Direct trust
  - Hierarchical trust
  - Web of trust (by PGP)