MAKALAH

DIGITAL SIGNATURE

Disusun Untuk Memenuhi Tugas Mata Kuliah

Sekuriti Komputer

Disusun oleh :

NAMA : FAUZAN BEKTI NUGOHO

NIM : 3085113013

Dosen Pengampu :

IKRIMACH, S.Kom

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS TEKNOLOGI YOGYAKARTA

2009

KATA PENGANTAR

Segala puji dan syukur kami panjatkan kehadirat Allah S.W.T yang telah memberikan berkah, rahmat dan hidayah-Nya kepada kami sehingga kami dapat menyelesaikan penulisan makalah yang berjudul Digital Signature ini. Tak lupa shalawat dan salam semoga senantiasa tercurah kepada junjungan dan tauladan kita, Rasulullah Muhammad S.A.W, keluarga dan para sahabatnya serta seluruh pengikutnya.

Tanda tangan digital bukanlah seperti bayangan orang awan yang (mungkin) berpikiran bahwa tanda tangan digital adalah tanda tangan asli seseorang yang di scan dan ditampilkan di dalam dokumen yang kita upload atau kita kirimkan kepada seseorang melalui internet atau pengiriman file dengan menggunakan media penyimpanan digital (disk storge). Tanda tangan digital muncul akibat keresahan orang ketika akan mengirimkan dokumen yang penting… muncul pikiran apakah file yang dikirimkan tersebut tidak mengalami perubahan ketika dikirimkan dan isinya sangat berbeda sekali ketika diterima oleh penerima dokumen, tapi apabila si pengirim mencantumkan tanda tangan digital pada dokumen itu, si penerima dapat meyakini bahwa setelah ditandatangani pengirim, dokumen itu tidak ada yang memanipulasi pada saat menjalani proses pengiriman.

Kami menyadari bahwa penulisan makalah ini masih jauh dari sempurna dan masih terdapat banyak kekurangan karena segala keterbatasan yang kami miliki. Oleh karena itu, dengan segala kerendahan hati, saran dan kritik yang membangun sangat kami harapkan demi kesempurnaan penulisan makalah ini.

Yogyakarta, November 2009

Fauzan Bekti Nugroho

DAFTAR ISI

BAB I
PENDAHULUAN

A. LATAR BELAKANG

Dengan seiring berkembangnya zaman yang semakin maju, perkembangan teknologi pun seiring dengan perkembangan zaman tesebut. Perekembangan teknologi tersebut juga berpengaruh pada kemajuan teknologi dalam dunia IT (Information Technologi) yang juga berkembang dengan pesat. Dengan merebaknya email palsu yang mencatut identitas seseorang, baik yang dihasilkan oleh program seperti halnya *worm*, atau memang dilakukan oleh pihak tertentu, penggunaan teknik autentifikasi pesan menjadi lebih diperlukan. Seperti halnya surat yang pengirimannya tinggal dimasukkan ke dalam kotak pos yang banyak dijumpai di pinggir jalan, server email juga menerima pesan yang akan dikirimkan serupa itu. Autentifikasi umumnya hanya dilakukan terhadap alamat IP komputer pengirim, dan sepanjang alamat tadi dianggap valid, maka siapapun dapat menulis email dari komputer tersebut.

Kita dapat menerima surat yang datang lewat tukang pos dan di dalamnya mengatasnamakan siapapun. Karena memang tukang pos tidak berkepentingan dengan validitas isi surat tersebut. Tugas utama dia adalah mengantarkan surat ke alamat tujuan, tanpa memedulikan siapapun pengirimnya. Adalah tanggung jawab pengirim surat untuk menandai surat tersebut sehingga dapat dipercaya (*trusted*) bahwa memang pesan yang ditulis berasal darinya. Sedangkan di sisi penerima pesan, harus terdapat sebuah cara sehingga dia dapat mengetahui identitas pengirim pesan dan cukup yakin bahwa pesan tersebut memang ditulis oleh yang bersangkutan.

Cara yang digunakan di atas kertas: dituliskan tanda tangan atau stempel yang menunjukkan validitas pengirim pesan. Demikianlah tanda tangan digital (*digital signature*) juga dimaksudkan seperti itu. Tanda tersebut harus unik untuk membedakan satu pengirim dengan lainnya, sulit ditiru pihak lain, dan dapat menjaga integritas pesan yang ditandai. Tujuannya adalah menghindari pencatutan

identitas dan pengubahan pesan oleh pihak ketiga di tengah jalan (*man in the middle attack*) pada saat pesan tersebut ditransmisikan. Pengubahan pesan digital lebih sulit terlihat dibanding pesan di atas surat.

Untuk keperluan yang penting ini, tersedia alat bantu yang dapat diperoleh secara cuma-cuma, yakni Pretty Good Privacy, PGP, dan GNU PGP, atau GPG. Tentu saja masih terdapat penyedia layanan tanda tangan digital lainnya, namun PGP dan GPG lebih dikenal luas dan GPG adalah produk Open Source. Untuk menggunakan PGP di luar Amerika Serikat, gunakan versi internasional, sedangkan GPG sendiri karena dikembangkan di luar wilayah hukum Amerika Serikat, maka bebas digunakan oleh siapapun. Restriksi ini berkaitan dengan aturan ekspor produk enkripsi yang berkait dengan pemakaian kunci sandi untuk pemakaian tanda tangan digital ini.

Karena tujuan pemakaian tanda tangan digital berbeda dengan enkripsi yang bersifat menyembunyikan, maka pesan tersebut tetap dapat terbaca oleh semua orang, namun di bagian bawahnya terdapat “tanda tangan” yang dapat digunakan untuk memeriksa integritas pesan dan validitas pengirimnya.

B. TUJUAN PENULISAN

Makalah ini ditulis dengan tujuan :

1. Tujuan Subjektif

   Guna Memperoleh nilai tugas dalam mata kuliah Sekuriti Komputer di Universitas Teknologi Yogyakarta.

2. Tujuan Objektif

   Dengan penulisan makalah ini diharapkan agar kita semua mengetahui tentang apa itu digital signature, apa kegunaan dan bagaimana cara penggunaannya.

BAB II
PEMBAHASAN KOMPUTER DAN KRIMINALITAS

A. TANDA TANGAN DIGITAL

Tanda tangan digital adalah pesan elektronik yang secara unik mengidentifikasi pengirim sebuah pesan.

1. Aktivitas Tanda Tangan Digital

Seperti telah disebutkan, teknik enkripsi kunci publik menjamin bahwa pesan telah terkirim dengan aman dan hal ini juga berlaku untuk transaksi-transaksi yang lainnya. Menggunakan teknologi ini, pengirim dan penerima pesan masing-masing memiliki dua kunci, yaitu kunci pribadi dan kunci publik. Kunci pribadi tidak akan diberitahukan kepada siapapun, sedangkan kunci publik akan diberitahukan kepada setiap orang. Selama melakukan proses enkripsi terhadap pesan dengan kunci publik penerima, membuat orang lain tidak bisa membaca apabila tidak memegang kunci pribadi untuk membuka pesan. Tanda tangan digital adalah pengganti tanda tangan secara manual yang bersifat elektronik dan mempunyai fungsi sama dengan tanda tangan manual. Tanda tangan digital juga merupakan rangkaian bit yang diciptakan dengan melakukan komunikasi elektronik melalui fungsi hash satu arah dan kemudian melakukan enkripsi pesan dengan kunci pribadi pengirim. Tanda tangan digital bukan merupakan gambar digital dari tanda tangan yang dibuat oleh tangan atau tanda tangan yang diketik. Tanda tangan digital mempunyai sifat yang unik untuk masing-masing dokumen itu sendiri dan beberapa perubahan pada dokumen akan menghasilkan tanda tangan digital yang berbeda. Tanda tangan digital dapat digunakan untuk tujuan yang sama seperti tanda tangan yang ditulis oleh tangan, yang didalamnya mungkin menandakan surat tanda terima, persetujuan atau tujuan keamanan informasi penting.

2. Aktivitas Tanpa Tanda Tangan Digital

Tanda tangan yang tidak menggunakan cara digital, hanyalah tanda tangan biasa yang dengan cara manual saja dan mengharuskan menggunakan alat tulis dan sangat berbeda dengan tanda tangan digital yang keamanan yang lebih terjamin dan juga dapat disimpan dengan menggunakan paswort yang hanya kita sendiri ketahui.

B. YANG MEMERLUKAN TANDA TANDA TANGAN DIGITAL

Macam-macam pengguna Tanda tangan digital antara laian digunakan di didalam bidang:

1. Pemerintah

RUU ITE yang mulai dibahas pada hari ini telah diperjuangkan cukup lama baik oleh kalangan pelaku IT, akademisi, dan pemerintah. Untuk sampai kepada naskah RUU ITE, pemerintah dengan mengundang pakar-pakar dibidang IT dan Cyber Law telah melakukan pengkajian tentang perlunya regulasi di bidang Cyber Law dan dituangkan ke dalam naskah akademik RUU ITE. Dari kajian yang telah dilakukan, disimpulkan bahwa yang diperlukan oleh Indonesia saat ini bentuk regulasi yang bersifat komprehensif mengingat saat ini Indonesia belum memiliki regulasi di bidang Cyber Law.

2. Individu

Ketika penerima mendapat komunikasi tertanda secara digital dalam bentuk yang dienkripsi, komputer yang sama dan fungsi hash yang pengirim gunakan untuk menciptakan tanda tangan digital dari program yang mengenkripsi tanda tangan yang secara otomatis menggunakan kunci publik pengirim. Oleh karena itu, jika program dapat mendekripsi tanda tangan, penerima tahu bahwa komunikasi datang dari pengirim, karena hanya kunci publik pengirim akan mendekripsi tanda tangan digital yang dienkripsikan dengan kunci pribadi pengirim.

3.Masyarakat

Dengan perkembangan teknologi informasi saat ini masyarakat kita semakin ingin menunjukkan rasa ingin tau yang tinggi, karena itu perkembangan teknologi dengan menggunakan tanda tangan digital ini mulai dikenal melalui dunia internet. Karena penggunaan tanda tangan digital harus unik sehingga dapat membedakan pengirim yang satu degan yang lainnya. Tanda tangan digital juga harus sulit untuk ditiru dan dipalsukan sehingga integritas dan keabsahan pesan dapatterjaga. Dengan demikian diharapkan pencatutan identitas ketika pesan atau email tersebut dikirim dapat dihindari. Tidak hanya pencatutan identitas yang diharapkan dapat dihindari dengan membubuhkan tanda tangan digital, tetapi juga pengubahan pesan oleh pihak yang tidak berhak. Hal ini disebabkan karena pengubahan pesan digital apalagi yang sudah dibubuhi tanda tangan digital lebih jauh sulit dibandingkan dengan mengubah pesan yang ditulis di atas kertas.

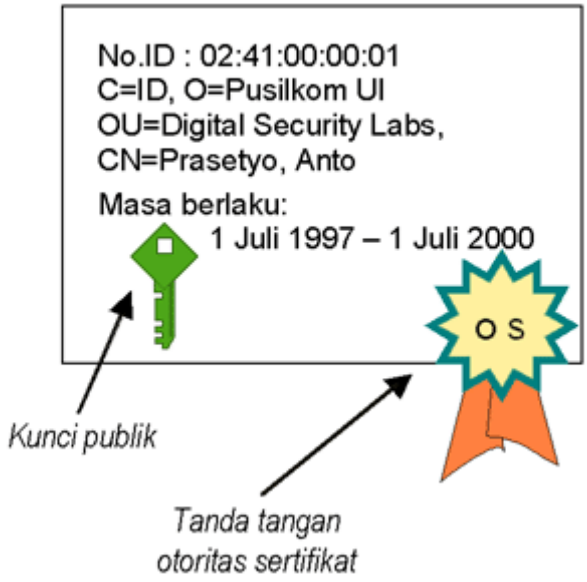
C. PENGGUNAAN TANDA TANGAN DIGITAL

Salah satu cara yang digunakan untuk memastikan surat tersebut adalah dengan mengecek tanda tangan yang ada di dalam surat tersebut dan stempel yang menunjukkan keaslian pengirim surat. Tanda tangan digital atau yang lebih dikenal dengan digital signature mempunyai fungsi yang sama dengan tanda tangan analog yang ditulis di atas kertas. Tanda tangan digital harus unik sehingga dapat membedakanpengirim yang satu degan yang lainnya. Tanda tangan digital juga harus sulit untuk ditiru dan dipalsukan sehingga integritas dan keabsahan pesan dapat terjaga. Dengan demikian diharapkan pencatutan identitas ketika pesan atau email tersebut dikirim dapat dihindari. Tidak hanya pencatutan Untuk keperluan yang penting ini, tersedia alat bantu yang dapat diperoleh secara cuma-cuma, yakni Pretty Good Privacy (PGP) dan Gnu Privacy Guard atau GPG. Tentu saja masih terdapat penyedia layanan tanda tangan digital lainnya, namun PGP dan GPG lebih dikenal luas. GPG adalah produk Open Source yang dapat diperoleh secara gratis tanpa harus membayar lisensi. Penggunaaan PGP di luar

Amerika Serikat harus menggunakan versi internasional. Sedangkan GPG sendiri karena dikembangkan di luar wilayah hukum Amerika Serikat, maka bebas digunakan oleh siapapun. Restriksi ini berkaitan dengan aturan ekspor produk enkripsi yang berkait dengan pemakaian kunci sandi untuk pemakaian tanda tangan digital ini [DIR04]. Penggunaan tanda tangan digital ini tidak terlalu sulit. Kedua belah pihak yang akan berkomunikasi harus menyiapkan sepasang kunci, yaitu kunci privat (private key) dan kunci publik (public key). Kunci privat hanya dipegang oleh pemiliknya sendiri. Sedangkan kunci publik dapat diberikan kepada siapapun yang memerlukannya.

D. HAMBATAN YANG TERJADI

Ada masalah dalam pendistribusian kunci publiknya. Katakanlah Anto hendak mengirim kunci publiknya (*PbA*) kepada Badu. Tapi saat kunci itu dikirim lewat jaringan publik, Maling mencuri kunci *PbA*. Kemudian Maling menyerahkan kunci publiknya (*PbM*) kepada Badu, sambil mengatakan bahwa kunci itu adalah kunci publik milik Anto. Badu, karena tidak pernah memegang kunci publik Anto yang asli, percaya saja saat menerima *PbM*. Saat Anto hendak mengirim dokumen yang telah ditandatanganinya dengan kunci privatnya (*PvA*) kepada Badu, sekali lagi Maling mencurinya. Tanda tangan Anto pada dokumen itu lalu dihapus, dan kemudian Maling membubuhkan tanda tangannya dengan kunci privatnya (*PvM*). Maling mengirim dokumen itu ke Badu sambil mengatakan bahwa dokumen ini berasal dari Anto dan ditandatangani oleh Anto. Badu kemudian memeriksa tanda tangan itu, dan mendapatkan bahwa tanda tangan itu sah dari Anto. Tentu saja *kelihatan* sah, karena Badu memeriksanya dengan kunci _ublic *PbM*, bukan dengan *PbA*.



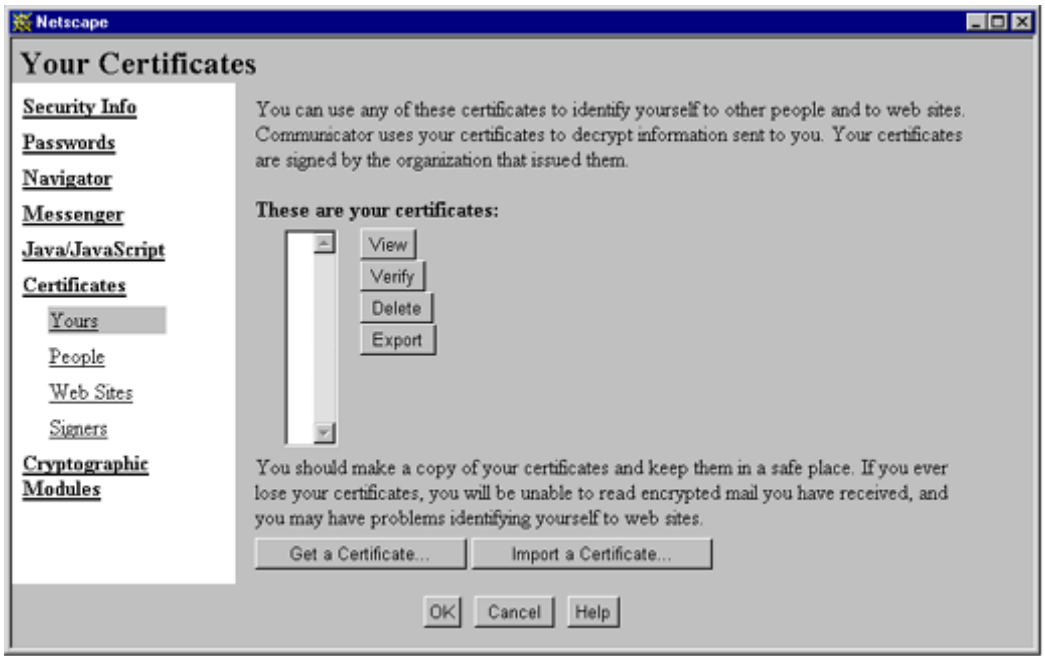
Gambar 1. Konsep sertifikat digital

E. SOLUSI

Untuk mengatasi masalah sekuriti pendistribusian kunci publik, maka kunci publik itu ‘direkatkan’ pada suatu sertifikat digital. Sertifikat digital selain berisi kunci publik juga berisi informasi lengkap mengenai jati diri pemilik kunci tersebut, sebagaimana layaknya KTP, seperti nomor seri, nama pemilik, kode negara/perusahaan, masa berlaku dsb. Sama halnya dengan KTP, sertifikat digital juga ditandatangani secara digital oleh lembaga yang mengeluarkannya, yakni otoritas sertifikat (OS) atau *certificate authority* (CA). Dengan menggunakan kunci public dari suatu sertifikat digital, pemeriksa tanda tangan dapat merasa yakin bahwa kunci publik itu memang berkorelasi dengan seseorang yang namanya tercantum dalam sertifikat digital itu.

Gambar 2. Dialog box untuk membuat sertifikat digital pada Microsot Outlook

Kini Internet tools versi terbaru dari Microsoft dan Netscape sudah menyediakan fasilitas bagi penggunaan sertifikat digital user. Dengan Outlook Express dari Microsoft Internet Explorer 4.0 misalnya, kita bisa memesan suatu sertifikat digital melalui menu Tools Options Security, lalu mengklik [Get Digital ID…]. Sedangkan pada Netscape Communicator 4.0, hal serupa dilakukan dengan menekan tombol Security pada toolbar, lalu mengklik Certificate Yours, lantas mengklik tombol [Get A Certificate…]. Sertifikat yang didapatkan itu kemudian disimpan di hard disk, dan diproteksi dengan password. Patut dicatat bahwa teknologi kunci publik dan sertifikat digital pada kedua produk ini juga dipergunakan untuk melakukan proses merahasiakan/menyandikan data, sehingga tidak ada pihak ketiga yang bisa membaca data yang sedang dikirimkan.



Gambar 3. Dialog box untuk membuat sertifikat digital pada Netscape Communicator

Sebenarnya perkakas terbaik yang digunakan untuk membuat tanda tangan digital adalah *smart card.* Di dalam smart card tersimpan kunci privat dan sertifikat digital, namun yang bisa dikeluarkan dari smart card hanya sertifikat digital saja (untuk keperluan verifikasi tanda tangan). Sedangkan kunci privat tidak bisa diintip oleh apapun dari luar smartcard, karena hanya dipakai untuk proses penandatanganan yang dilakukan di dalam smart card.

F. TINGKAT KEGAGALAN

Tetapi sayangnya ada satu hal yang terlupa, bahwa pada dunia komputasi manipulasi terhadap program dan sabotase terhadap komputer pengguna bukanlah hal yang sulit dilakukan. Seseorang bisa saja menyabotase komputer orang lain untuk menandatangani dokumen tanpa sepengetahuan orang yang bersangkutan. Dengan kata lain, tanda-tangan digital hanya memberikan otentikasi antara dokumen dengan komputer, tetapi tidak memberikan otentikasi keterkaitan antara komputer dengan pemilik kunci privat yang sah. Jika seseorang berada di

pengadilan dan ditanya tentang tanda-tangan digital miliknya pada sebuah dokumen, dia dapat saja mengatakan bahwa ia tidak pernah menandatangani dokumen tersebut, dan ketika saksi ahli dihadirkan ia akan menjelaskan bahwa mungkin saja dokumen diberi tandatangan digital tanpa sepengetahuan si pemilik kunci privat.

BAB III
PENUTUP

A. KESIMPULAN

Apabila ada perubahan pada karakter individual dalam dokumen aslinya, nilai dalam intisari juga akan berubah. Ciri ini merupakan alat untuk memastikan bahwa isi dokumen bisnis tidak diubah atau dirusak selama masa pengiriman. Digital Certificate: Melakukan identifikasi pemilik dari kunci pribadi tertentu dan kunci publiknya yang sesuai, serta memastikan waktu validitas sertifikasinya. Sertifikasi digital dikeluarkan oleh pihak ketiga yang handal, yaitu yang disebut sebagai pihak yang berwenang untuk memberikan sertifikasi, seperti : Verisign, Entrust, Digital Signature Trust Tanda tangan digital pihak yang berwenang untuk memberikan sertifikasi juga dimasukkan ke dalam sertifikasi digital agar validasi sertifikat dapat diverifikasi.

DAFTAR PUSTAKA

Ikhlasul Amal.http://www.tanda-tangan.com/
http://id.wikipedia.org