Otentikasi Dokumen Elektronik Menggunakan Tanda Tangan Digital

Ronald Makaleo Tandiabang, Tomy Handaka Patria, Anang Barnea

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : 1f19034@students.if.itb.ac.id, if19046@students.if.itb.ac.id,
if19050@students.if.itb.ac.id

Abstrak

Dalam dunia nyata, untuk menjamin keaslian serta legalitas suatu dokumen digunakan tanda tangan. Tanda tangan ini merupakan suatu tanda yang bersifat unik milik seseorang dan digunakan untuk memberi pengesahan bahwa orang tersebut setuju dan mengakui isi dari dokumen yang ditandatangani. Untuk dokumen-dokumen elektronik pun dibutuhkan hal semacam ini. Oleh karena itu, diciptakan suatu sistem otentikasi yang disebut tanda tangan digital. Tanda tangan digital merupakan suatu cara untuk menjamin keaslian suatu dokumen elektronik dan menjaga supaya pengirim dokumen dalam suatu waktu tidak dapat menyangkal bahwa dirinya telah mengirimkan dokumen tersebut. Tanda tangan digital menggunakan algoritma-algoritma serta teknik-teknik komputer khusus dalam penerapannya.

***Kata kunci**: digital signature, information authentication, cryptography, information security, nonrepudiation*

1. Pendahuluan

Dewasa ini, kebutuhan akan kerahasiaan informasi serta penjagaan atas keaslian suatu informasi dirasa semakin meningkat. Pembentukan *framework* untuk otentikasi dari informasi berbasis komputer memerlukan pengetahuan dan ketrampilan akan hukum dan bidang keamanan komputer. Akan tetapi, mengkombinasikan antara kedua hal ini bukan pekerjaan yang mudah. Konsep yang ada di dunia hukum seringkali hanya berkorelasi sedikit dengan konsep yang ada pada dunia keamanan komputer. Sebagai contoh, konsep "tanda tangan digital" (*digital signature*) yang dikenal pada dunia keamanan komputer adalah hasil dari penerapan teknik-teknik komputer pada suatu informasi. Sedangkan di dunia umum, tanda tangan mempunyai arti yang lebih luas, yaitu sebarang tanda yang dibuat dengan maksud untuk melegalisasi dokumen yang ditandatangani.

2. Tanda Tangan dan Hukum

Secara umum, penandatanganan suatu dokumen bertujuan untuk memenuhi keempat unsur di bawah ini[1]:

1. **Bukti**: Sebuah tanda tangan mengotentikasikan suatu dokumen dengan mengidentifikasikan penandatangan dengan dokumen yang ditandatangani.

2. **Formalitas**: Penandatanganan suatu dokumen ‘memaksa’ pihak yang menandatangani untuk mengakui pentingnya dokumen tersebut.
3. **Persetujuan**: Dalam beberapa kondisi yang disebutkan dalam hukum, sebuah tanda tangan menyatakan persetujuan pihak yang menandatangani terhadap isi dari dokumen yang ditandatangani.
4. **Efisiensi**: Sebuah tanda tangan pada dokumen tertulis sering menyatakan klarifikasi pada suatu transaksi dan menghindari akibat-akibat yang tersirat di luar apa yang telah dituliskan.

Kebutuhan-kebutuhan formal dari suatu transaksi legal, termasuk kebutuhan akan tanda tangan, berbeda-beda dalam setiap sistem hukum legal dan rentang waktu tertentu. Meskipun hal-hal alamiah mengenai suatu transaksi tidak berubah, hukum hanya memulai untuk mengadaptasi terhadap teknologi mutakhir.

Untuk mencapai tujuan dari penandatanganan suatu dokumen seperti di atas, sebuah tanda tangan harus mempunyai atribut-atribut berikut:

1. **Otentikasi Penanda tangan**: Sebuah tanda tangan seharusnya dapat mengindentifikasikan siapa yang menandatangani dokumen tersebut dan susah untuk ditiru orang lain.
2. **Otentikasi Dokumen:** Sebuah tanda tangan seharusnya mengidentifikasikan apa yang ditandatangani, membuatnya tidak mungkin dipalsukan ataupun diubah (baik dokumen yang ditandatangani maupun tandatangannya) tanpa diketahui.

Otentikasi penandatangan dan dokumen adalah alat untuk menghindari pemalsuan dan merupakan suatu penerapan konsep “*nonrepudiation*” dalam bidang keamanan informasi. *Nonrepudiation* adalah jaminan dari keaslian ataupun penyampaian dokumen asal untuk menghindari penyangkalan dari penandatangan dokumen (bahwa dia tidak menandatangani dokumen tersebut) serta penyangkalan dari pengirim dokumen (bahwa dia tidak mengirimkan dokumen tersebut).

3. Cara Kerja Teknologi Tanda Tangan Digital

Tanda tangan digital dibuat dengan menggunakan teknik kriptografi, suatu cabang dari matematika terapan yang menangani tentang pengubahan suatu informasi menjadi bentuk lain yang tidak dapat dimengerti dan dikembalikan seperti semula. Tanda tangan digital menggunakan “*public key cryptography*” (kriptografi kunci publik), dimana algoritmanya menggunakan dua buah kunci, yang pertama adalah kunci untuk membentuk tanda tangan digital atau mengubah data ke bentuk lain yang tidak dapat dimengerti, dan kunci kedua digunakan untuk verifikasi tanda tangan digital ataupun mengembalikan pesan ke bentuk semula. Konsep ini juga dikenal sebagai “*assymmetric cryptosystem*” (sistem kriptografi non simetris).

Sistem kriptografi ini menggunakan kunci privat, yang hanya diketahui oleh penandatangan dan digunakan untuk membentuk tanda tangan digital, serta kunci publik, yang digunakan untuk verifikasi tanda tangan digital. Jika beberapa orang ingin memverifikasi suatu tanda tangan digital yang dikeluarkan oleh seseorang, maka kunci publik tersebut harus disebarkan ke orang-orang tersebut. Kunci privat dan kunci publik ini sesungguhnya secara matematis ‘berhubungan’ (memenuhi persamaan-persamaan dan kaidah-kaidah tertentu). Walaupun demikian, kunci privat tidak dapat ditemukan menggunakan informasi yang didapat dari kunci publik.

Proses lain yang tak kalah penting adalah “fungsi hash”, digunakan untuk membentuk sekaligus memverifikasi tanda tangan digital. Fungsi hash adalah sebuah algoritma yang membentuk representasi digital atau semacam “sidik jari” dalam bentuk “nilai hash” (*hash value*) dan biasanya jauh lebih kecil dari dokumen aslinya dan unik hanya berlaku untuk dokumen tersebut. Perubahan sekecil apapun pada suatu dokumen akan mengakibatkan perubahan pada “nilai hash” yang berkorelasi dengan dokumen tersebut. Fungsi hash yang demikian disebut juga “fungsi hash satu arah”, karena suatu nilai hash tidak dapat digunakan untuk membentuk kembali dokumen aslinya. Oleh karenanya, fungsi hash dapat digunakan untuk membentuk tanda tangan digital. Fungsi hash ini akan menghasilkan “sidik jari” dari suatu dokumen (sehingga unik hanya berlaku untuk dokumen tersebut) yang ukurannya jauh lebih kecil daripada dokumen aslinya serta dapat mendeteksi apabila dokumen tersebut telah diubah dari bentuk aslinya.

Penggunaan tanda tangan digital memerlukan dua proses, yaitu dari pihak penandatangan serta dari pihak penerima. Secara rinci kedua proses tersebut dapat dijelaskan sebagai berikut:

1. **Pembentukan tanda tangan digital** menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat yang telah didefinisikan sebelumnya. Untuk menjamin keamanan nilai hash maka seharusnya terdapat kemungkinan yang sangat kecil bahwa tanda tangan digital yang sama dapat dihasilkan dari dua dokumen serta kunci privat yang berbeda.
2. **Verifikasi tanda tangan digital** adalah proses pengecekan tanda tangan digital dengan mereferensikan ke dokumen asli dan kunci publik yang telah diberikan, dengan cara demikian dapat ditentukan apakah tanda tangan digital dibuat untuk dokumen yang sama menggunakan kunci privat yang berkorespondensi dengan kunci publik.

Untuk menandatangani sebuah dokumen atau informasi lain, penandatangan pertama-tama membatasi secara tepat bagian-bagian mana yang akan ditandatangani. Informasi yang dibatasi tersebut dinamakan “*message*”. Kemudian aplikasi tanda tangan digital akan membentuk nilai hash menjadi tanda tangan digital menggunakan kunci privat. Tanda tangan digital yang terbentuk adalah unik baik untuk *message* dan juga kunci privat.

Umumnya, sebuah tanda tangan digital disertakan pada dokumennya dan juga disimpan dengan dokumen tersebut juga. Bagaimanapun, tanda tangan digital juga dapat dikirim maupun disimpan sebagai dokumen terpisah, sepanjang masih dapat diasosiasikan dengan dokumennya. Karena tanda tangan digital bersifat unik pada dokumennya, maka pemisahan tanda tangan digital seperti itu merupakan hal yang tidak perlu dilakukan.

Proses pembentukan dan verifikasi tanda tangan digital memenuhi unsur-unsur paling penting yang diharapkan dalam suatu tujuan legal, yaitu:

1. **Otentikasi Penandatangan:** Jika pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah yang telah didefinisikan, maka tanda tangan digital akan dapat menghubungkan/mengasosiasikan dokumen dengan penandatangan. Tanda tangan digital tidak dapat dipalsukan, kecuali penandatangan kehilangan kontrol dari kunci privat miliknya.
2. **Otentikasi Dokumen:** Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan tingkat kepastian dan ketepatan yang jauh lebih tinggi daripada tanda tangan di atas kertas.

3. **Penegasan:** Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan. Tindakan ini dapat menegaskan bahwa penandatangan setuju dan bertanggung jawab terhadap isi dokumen.
4. **Efisiensi:** Proses pembentukan dan verifikasi tanda tangan digital menyediakan tingkat kepastian yang tinggi bahwa tanda tangan yang ada merupakan tanda tangan sah dan asli dari pemilik kunci privat. Dengan tanda tangan digital , tidak perlu ada verifikasi dengan melihat secara teliti (membandingkan) antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya seperti yang biasa dilakukan dalam pengecekan tanda tangan secara manual.

4. Kelemahan dan Keunggulan Tanda Tangan Digital

Kelemahan yang masih menyertai teknologi tanda tangan digital adalah:

1. **Biaya tambahan secara institusional:** Tanda tangan digital memerlukan pembentukan otoritas-otoritas yang berhak menerbitkan sertifikat serta biaya-biaya lain untuk menjaga dan mengembangkan fungsi-fungsinya.
2. **Biaya langganan:** Penanda tangan memerlukan perangkat lunak aplikasi dan juga membayar untuk memperoleh sertifikasi dari otoritas yang berhak mengeluarkan sertifikat.

Sedangkan kelebihan yang paling utama dari adanya tanda tangan digital adalah lebih terjaminnya otentikasi dari sebuah dokumen. Tanda tangan digital sangat sulit dipalsukan dan berasosiasi dengan kombinasi dokumen dan kunci privat secara unik[2].

5. Kesimpulan

Tanda tangan digital merupakan teknik yang sangat tepat digunakan untuk menjamin keaslian suatu dokumen serta menghindari adanya penyangkalan bahwa seseorang telah menandatangani suatu dokumen. Teknik ini jauh lebih canggih dan lebih efisien daripada tanda tangan yang dilakukan secara manual.

[1] J. M. Perillo, *The Statute of Frauds in the Light of theFunctions and Disfunctions of Form*, Fordham L. Rev. 39, 48-641974.
[2] B. Schneier, *Applied Cryptography*, 403-410, John Wiley & Sons, 1996.