# Tanda Tangan Digital Pada Catatan Medis Elektronik

Muhammad Iqbal 13510064
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*13510064@std.stei.itb.ac.id*

***Abstract*— Penggunaan Sistem Informasi Kesehatan merupakan hal yang penting di setiap organisasi kesehatan yang membutuhkan integrasi dan sentralisasi informasi medis pasien. Pertukaran informasi secara digital menyediakan metoda yang lebih cepat dan dapat diandalkan serta mendukung manajemen informasi yang baik, namun di sisi yang lain komunikasi digital ini dapat menimbulkan risiko keamanan yang serius. Risiko keamanan yang serius ini disebabkan oleh fakta bahwa setiap modifikasi dan keterbukaan data medis pasien pada pihak yang tidak berwenang dapat menghilangkan nyawa manusia. Oleh karena itu, elemen keamanan data seperti confidentiality, integrity, non-repudiation, availability, dan accountability merupakan kebutuhan yang bersifat wajib. Pada makalah ini penulis mencoba menerapkan tanda tangan digital untuk meningkatkan integritas informasi catatan medis.**

***Index Terms*—tanda tangan digital, sistem informasi kesehatan, catatan medis, kriptografi**

## I. PENDAHULUAN

Perkembangan teknologi informasi yang sangat drastis telah mempengaruhi ke berbagai bidang termasuk kesehatan. Masyarakat sadar bahwa teknologi informasi merupakan adalah hal penting dalam peradaban manusia untuk mengatasi masalah derasnya arus informasi. Di dunia medis, dengan perkembangan pengetahuan yang begitu cepat dokter akan cepat tertinggal jika tidak memanfaatkan berbagai hal untuk mengupdate perkembangan terbaru.

Catatan medis elektronik adalah salah satu tantangan besar dalam penerapan teknologi informasi dan komunikasi di rumah sakit, yaitu penerapan catatan medis berbasis komputer. Pengertian catatan medis berbasis komputer bervariasi, akan tetapi, secara prinsip adalah penggunaan database untuk mencatat semua data medis, demografis serta setiap kejadian dalam manajemen pasien di rumah sakit maupun di klinik. Catatan medis berbasis komputer akan menghimpun berbagai data klinis pasien baik yang berasal dari hasil pemeriksaan dokter, digitasi dari alat diagnosis, konversi hasil pemeriksaan laboratorium maupun interpretasi klinis. Catatan medis berbasis komputer yang lengkap biasanya disertai dengan fasilitas sistem pendukung keputusan (SPK) yang memungkinkan pemberian bantuan diagnosis maupun terapi agar dokter maupun klinisi dapat mematuhi protokol klinik.

Pada dasarnya catatan medis elektronik adalah penggunaan metode elektronik untuk pengumpulan, penyimpanan, pengolahan serta pengaksesan catatan medis pasien di rumah sakit yang telah tersimpan dalam suatu sistem manajemen basis data multimedia yang menghimpun berbagai sumber data medis. Jenis data catatan medis dapat berupa teks (baik yang terstruktur maupun naratif), gambar digital (jika sudah menerapkan radiologi digital), suara (misalnya suara jantung), video maupun yang berupa biosignal seperti catatanan EKG.

Perkembangan teknologi catatan medis di Indonesia cenderung lambat. Salah satu penyebabnya adalah seringnya muncul pertanyaan bagaimana keabsahan dokumen elektronik, karena jika terjadi kesalahan dalam informasi pada catatan medis, maka akan berakibat sangat fatal pada masa depan pasien.

Untuk menangani masalah keraguan akan keabsahan dokumen catatan medis ini, maka tanda tangan digital merupakan salah satu metode yang tepat. Dengan digunakannya tanda tangan digital oleh pihak yang bertanggungjawab, maka keabsahan dokumen dapat dengan mudah diperiksa. Pengubahan dokumen oleh pihak yang bertanggungjawab dapat dideteksi. Dengan menggunakan tanda tangan digital, maka integritas data dari catatan medis dapat dipertahankan.

## II. DASAR TEORI

### *A. Catatan Medis*

Dalam penjelasan Pasal 46 ayat (1) UU Praktik Kedokteran yang dimaksud dengan rekam medis adalah berkas yang berisi catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien.

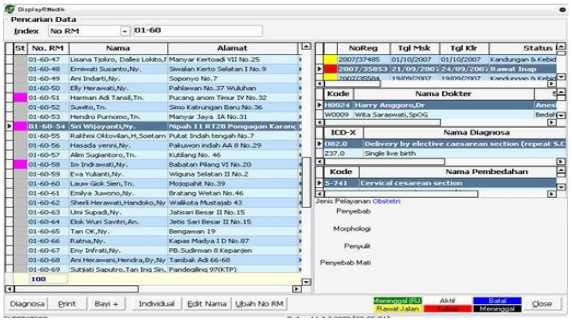
Dalam Peraturan Menteri Kesehatan Nomor 749a/Menkes/Per/XII/1989 tentang Rekam Medis dijelaskan bahwa rekam medis adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain kepada pasien pada sarana pelayanan kesehatan..

Yang berkewajiban membuat rekam medis adalah tenaga kesehatan:

1. Tenaga medis meliputi dokter dan dokter gigi

2. Tenaga keperawatan meliputi perawat dan bidan.
3. Tenaga kefarmasian meliputi apoteker, analis farmasi dan asisten apoteker.
4. Tenaga kesehatan masyarakat meliputi epidemiolog kesehatan, entomolog kesehatan, mikrobiologi kesehatan, penyuluh kesehatan, administrator kesehatan dan sanitarian.
5. Tenaga gizi meliputi nutrisionis dan dietisien.
6. Tenaga keterapian fisik meliputi fisioterapis, okupasiterapis dan terapis wicara.
7. Tenaga keteknisian medis meliputi radiografer, radioterapis, teknisi gigi, teknisi elektromedis, analisi kesehatan, refraksionis optisien, othotik prostetik, teknisi tranfusi dan perekam medis.

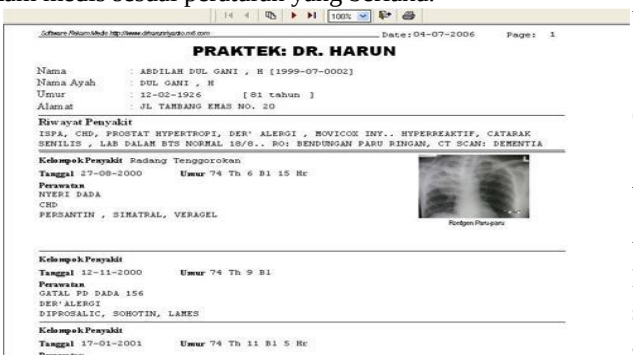
Rekam medis juga diartikan secara lebih luas adalah catatan dan data sebagai akibat hubungan langsung maupun tidak langsung dengan segala aktifitas di rumah sakit yang berkaitan dengan pengobatan pasien.



*Gambar 1 Contoh register rekam medis pasien secara elektronik*

Rekam Medis harus dibuat secara tertulis, lengkap dan jelas dan dalam bentuk teknologi Informasi elektronik yang diatur lebih lanjut dengan peraturan tersendiri.

Rekam medis terdiri dari catatan-catatan data pasien yang dilakukan dalam pelayanan kesehatan. Catatan-catatan tersebut sangat penting dalam pelayanan bagi pasien karena dengan data yang lengkap dapat memberikan informasi dalam menentukan keputusan, baik pengobatan, penanganan, tindakan medis dan lainnya. Dokter atau dokter gigi diwajibkan membuat rekam medis sesuai peraturan yang berlaku.




*Gambar 2 Contoh data rekam medis pada praktek mandirri dokter*

Mamfaat dari rekam medik elektronik/digital, yaitu :

- Kemudahan penelusuran dan pengiriman informasi
- Bisa dikaitkan dengan informasi lain yang berasal dari luar rekam medik
- Penyimpanan lebih ringkas
- Data dapat ditampilkan dengan cepat sesuai kebutuhan
- Abstraksi, pelaporan lebih mudah bahkan otomatis
- Kualitas data dan standar dapat dikendalikan
- Dapat diintegrasikan dengan perangkat lunak pendukung keputusan

Selain lebih baik dalam proses penggunaannya jika dibandingkan dengan rekam medik kartu, rekaman medik elektronik/digital tidaklah sempurna,juga terdapat hambatan dalam proses penggunaannya, yaitu:

- Kepercayaan terhadap komputer: keterandalan, privasi, keamanan
- Pemanfaatan untuk keperluan klinik sehari-hari (perlu waktu untuk analisis)
- Technophobia: sikap negatif atau gagap teknologi terhadap komputer di tempat kerja

Hal- hal yang dapat disimpan dalam rekam medik elektronik:

- Teks (kode, narasi, report)
- Gambar (komputer grafik, gambar yang di-scan, hasil foto rontgen digital)
- Suara (suara jantung, suara paru)
- Video (proses operasi

*B. Tanda Tangan Digital*

Pada beberapa kasus seringkali otentikasi yang diperlukan tetapi kerahasiaan pesan tidak. Maksudnya, pesan tidak perlu dienkripsikan, sebab yang dibutuhkan hanya keotentikan pesan saja. Kebutuhan tersebut dapat dipenuhi dengan pemberian tandatangan digital.

Algoritma kunci-publik dan fungsi hash dapat digunakan untuk kasus seperti ini. Tandatangan digital adalah suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan.

Pada Agustus 1991, NIST (The National of Standart and Technology) mengumumkan standard untuk tandatangan digital yang dinamakan Digital Signature Standard (DSS) yang terdiri dari dua komponen :

a. Algoritma tandatangan digital yang disebut DSA (Digital Signature Algorithm)

b. Fungsi Hash yang disebut SHA ( Secure Hash Algorithm)

Jadi DSA untuk penandatanganan pesan dan SHA untuk membangkitkan message digest dari pesan. Langkah-langkah pada proses tandatangan digital sebagai berikut:

a. Menentukan parameter DSA yaitu:

1. p adalah bilangan prima dengan panjang L bit, dimana $2^{L-1} < p < 2^{L}$ dengan $512 \leq L \leq 1024$ dan L adalah kelipatan 64. q, bilangan prima 160 bit, faktor dari p-1 dimana $2^{159} < q < 2^{160}$. Parameter p

bersifat publik.

2. $g = h^{(p-1)/q} \bmod p$, dimana $1 < h < p-1$ sehingga $g > 1$.Parameter g bersifat publik.
3. x bilangan bulat yang dibangkitkan random atau pseudorandom dimana $0 < x < q$ dengan panjang 160 bit. Parameter x bersifat privat.
4. $y = gx \bmod p$ adalah kunci publik
5. M adalah pesan yang akan diberi tandatangan
6. k = bilangan bulat yang dibangkitkan random atau pseudorandom dimana $0 < k < q$.

Parameter p, q dan g bersifat publik dan dapat digunakan bersama dalam sekelompok orang. Parameter p, q dan g juga bernilai tetap untuk periode/ waktu tertentu. Parameter x dan k hanya digunakan untuk pembangkitan tandatangan dan harus dijaga kerahasiaannya. Parameter k harus berbeda untuk setiap tandatangan.

b. Pembangkitan sepasang kunci :

1. Pilih bilangan prima p dan q, dimana $(p-1) \bmod q = 0$
2. Hitung $g = h(p-1)/q \bmod p$, dimana $1 < h < p-1$ dan $g > 1$
3. Tentukan kunci privat $x < q$
4. Hitung kunci publik $y = gx \bmod p$

   Jadi didapatkan kunci publik (p,q,g,y) dan kunci privat (p,q,g,x)

c. Pembangkitan tandatangan (signing) :

1. Ubah pesan m menjadi massage digest dengan fungsi Hash SHA

   menghasilkan SHA(M)
2. Tentukan bilangan acak $k < q$
3. Tanda tangan dari pesan m adalah bilangan r dan s yang didapat dari :

   $r = (g^k \bmod p) \bmod q$

   $s = (k^{-1} (SHA(M) + xr)) \bmod q$, $k^{-1}$ adalah invers dari k modulo q.

   Pada perhitungan nilai s, 160-bit string SHA(M) dikonversi terlebih dahulu ke dalam. Jika tandatangan yang dihasilkan benar maka nilai r dan atau s tidak mungkin 0.
4. Kirim pesan beserta tandatangan r dan s

d. Verifikasi keabsahan tandatangan (verifying) :

Sebelum diverifikasi, harus dipastikan tersedianya kunci publik pengirim (y), nilai p, q dan g beserta pesan yang bertandatangan r dan s. Verifier memeriksa terlebih dahulu apakah $0 < r < q$ and $0 < s < q$ kemudian menghitung :

$w = s^{-1} \bmod q$

$u1 = (SHA(M)*w) \bmod q$

$u2 = (r*w) \bmod q$

$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q)$

Jika v = r maka tandatangan sah berarti tandatangan diverifikasi dan verifier

dapat memiliki keyakinan yang tinggi bahwa pesan yang diterima dikirim oleh pihak memegang kunci rahasia x sesuai dengan y kunci publiknya, dengan kata lain pesan masih asli dan dokumen dikirim oleh pengirim yang benar.

Jika v tidak sama r, maka pesan tersebut mungkin telah dimodifikasi, pesan tersebut mungkin telah salah ditandatangani oleh penandatangan, atau pesan mungkin telah ditandatangani oleh pihak lain (bukan penandatangan sebenarnya) berarti pesan tidak valid. Berikut ini diberikan contoh perhitungan DSA:

a. Pembangkitan sepasang kunci

1. Pilih bilangan prima p dan q dengan $(p-1) \bmod q = 0$, yaitu p = 59419 dan q = 3301 (memenuhi 3301.18 = 59419-1)
2. Hitung $g = h(p-1)/q \bmod p$, dimana $1 < h < p-1$ dan $g > 1$, yaitu (ambil h = 100) $g = 100(59419-1)/3301 \bmod 59419 = 18870$
3. Tentukan kunci rahasia x bilangan bulat < q, ambil x = 3223
4. Hitung kunci publik $y = gx \bmod p = 188703223 \bmod 59419 = 29245$

b. Pembangkitan tandatangan (signing)

1. Hitung nilai hash dari pesan, misal H(m) = 4321
2. Tentukan bilangan acak $k < q$, misal diambil k = 997, $k.k^{-1} = 1 \bmod q$,

   didapat $k^{-1} = 2907$
3. Hitung r dan s sebagai berikut :

   $r = (gk \bmod p) \bmod q = (18870997 \bmod 59419) \bmod 3301 = 848$ $s = (k^{-1} (H(m) + x r)) \bmod q = (2907( 4321+3223. 848)) \bmod 3301 = 183$
4. Kirim pesan m dan tandatangan r dan s

c. Verifikasi keabsahan tandatangan

1. Hitung

   $w = s^{-1} \bmod q$

   $s.s^{-1} = 1 \bmod q$ didapat $s^{-1} = 469$

   $w = 469 \bmod 3301 = 469$

   $u1 = (H(m)*w) \bmod q = (4321. 469) \bmod 3301 = 3036$

   $u2 = (r*w) \bmod q = (848. 469) \bmod 3301 = 1592$

   $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q) = ((188703036 . 292451592 ) \bmod 59419) \bmod 3301 = 848$
2. Karena v = r maka tanda tangan sah.

## III. ANALISIS SOLUSI PERMASALAHAN

Didalam ruang lingkup permasalahan catatan medis elektronik, tanda tangan digital akan digunakan untuk menjamin keabsahan dokumen dalam setiap pertukaran informasi.

Hasil print-out dokumen medis fisik akan ditandatangani secara manual oleh pihak *signer*, lalu dengan proses pemindaian, tanda tangan ini akan diproses menjadi gambar yang nantinya akan diambil kode string. Kode string ini akan digunakan sebagai nilai SEED untuk membangkitkan parameter dan sepasang kuncu yaitu kunci privat dan kunci publik. Kunci publik didapatkan dari kunci privat yang ada. Sepasang kunci tersebut digunakan pada pembangkitan tandatangan digital.

Dokumen yang telah diberi tanda tangan digital ini kemudian dikirim ke *verifier* untuk kemudian dilakukan proses verifikasi terhadap dokumen tersebut.

Langkah-langkah pembangkitan kunci dalam sistem ini:

1. Melakukan pemindaian pada berkas dokumen fisik yang telah ditandatangani.
2. Tandatangan manual yang telah ada akan diambil kode stringnya untuk dijadikan SEED.
3. Buat parameter DSA dengan menggunakan kode string SSL.
4. Buat kunci publik dan kunci privat dari parameter tersebut.
5. Akan didapatkan parameter P, Q, G, X, Y, kunci publik dan kunci privat.

Langkah-langkah penandatanganan digital :

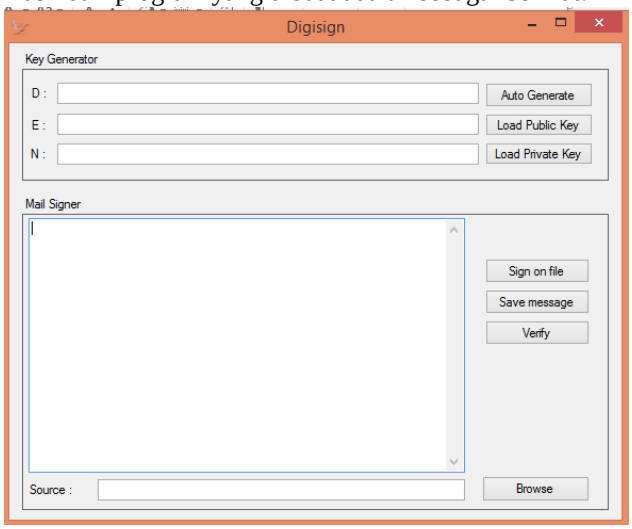
1. Ambil dokumen yang akan ditandatangani.
2. Lakukan fungsi *Hash* pada dokumen dengan menggunakan SHA-1
3. Ambil kunci privat.
4. Buat digital signature dengan menggunakan *Hash* dokumen dan kunci privat.
5. Didapatkan digital signature.
6. Selesai.

Langkah-langkah verifikasi dokumen:

1. Ambil dokumen yang telah ditandatangani.
2. Parse digital signature yang ada.
3. Verifikasi digital signature yang ada dengan menggunakan kunci publik.
4. Selesai.

## IV. HASIL PENGUJIAN

Hasil dari program yang dibuat adalah sebagai berikut:




*Gambar 3 Antar muka perangkat lunak*

Dengan menggunakan algoritma yang telah ditentukan sebelumnya, dilakukan pengujian dengan melakukan percobaan empat percobaan, dengan hasilnya dapat dilihat pada tabel dibawah:

| No | Nama File | Keterangan |
|---|---|---|
| 1 | Ttd1.jpg | Sah |
| 2 | Ttd2.jpg | Tidak Sah |
| 3 | Ttd3.jpg | Tidak Sah |
| 4 | Ttd4.jpg | Sah |

*Table 1 Hasil percobaan*

Dari hasil percobaan yang dilakukan, percobaan-percobaan yang tidak sah dilakukan dengan mengganti tanda tangan dan mengganti dokumen. Dari semua hasil, ketepatan pengujian keabsahan ini sudah mencapai 100%.

## V. KESIMPULAN

Dari hasil pengujian yang telah dilakukan, maka dapat disimpulkan beberapa hal berikut:

- Tandatangan digital dapat diterapkan pada catatan medis untuk menguji keabsahan dokumen.
- Metode yang dilakukan untuk membuat tandatangan digital pada dokumen sudah cukup efektif untuk mendeteksi keabsahan dokumen.

## VII. ACKNOWLEDGMENT

Penulis ingin mengucapkan terima kasih yang paling besar kepada Allah SWT. Dialah yang senantiasa memberikan kesehatan dan kesempatan bagi penulis sehingga bisa menyusun makalah ini hingga selesai. Alhamdulillah.

Ucapan terima kasih selanjutnya ingin penulis sampaikan kepada dosen mata kuliah IF4020, Bapak Rinaldi Munir. Berkat bimbingan beliau penulis bisa memahami ilmu-ilmu dalam bidang Kriptografi. Semoga kedepannya, ilmu ini akan terus bermanfaat bagi penulis dan orang-orang di sekitarnya.

Ucapan terima kasih terakhir diberikan kepada teman-teman sekelas penulis. Khususnya ucapan terima kasih yang sangat besar kepada rekan sekelompok tugas. Atas kerja samanya, tugas besar dan tugas kecil yang diberikan pada mata kuliah ini bisa dikerjakan dengan baik.

## REFERENSI

Depkes, R. I. (2006). Pedoman Penyelenggaraan dan Prosedur Rekam Medis Rumah Sakit di Indonesia. Revisi II.

Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 17(2), 281-308.

Merkle, R. C. (1990, January). A certified digital signature. In Advances in Cryptology—CRYPTO'89 Proceedings (pp. 218-238). Springer New York.

Munir, R. (2006). Kriptografi. Informatika, Bandung.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Mei 2014

ttd

Muhammad Iqbal 13510064