Autorisasi Tanda Tangan Digital dalam Organisasi

Amalfi Yusri Darusman 13507023
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If17023@students.if.itb.ac.id

Abstrak – Tanda tangan adalah satu-satunya bukti yang diakui sebagai otorisasi seseorang terhadap suatu dokumen yang valid. Dalam satu organisasi, otorisasi merupakan satu hal penting yang membatasi hak akses atau hak kelola suatu badan atau lembaga dalam organisasi tersebut. Pentingnya hak akses atau hak kelola tersebut dibatasi dengan tanda tangan seseorang yang berwenang. Namun ada kalanya sulit untuk mendapatkan tanda tangan yang berwenang ketika terpisah jarak maupun hal lainnya. Pengiriman lewat media digital (hasil scan tanda tangan) menjadi satu solusi, namun keamanan otorisasi tidak terjamin karena dapat disalahgunakan. Oleh karena itu, perlu adanya pembatasan akses terhadap media digital tersebut. Aplikasi ilmu kriptografi digunakan di sini sebagai pembatas otorisasi media digital tersebut, yang menggunakan konsep tanda tangan digital. Dengan demikian penggunaan media digital sebagai media distribusi tanda tangan dapat dikontrol.

Index Terms— hak akses, media digital, otorisasi, tanda tangan.

I. PENDAHULUAN

Tanda tangan adalah satu bentuk pemberian otorisasi seseorang kepada orang, lembaga atau badan yang bersangkutan, untuk melaksanakan sesuatu yang diizinkan oleh si pemberi tanda tangan. Dengan tanda tangan tersebut, si pemberi tanda tangan tidak perlu hadir di tempat ketika satu kegiatan dilakukan. Selain itu, tanda tangan jug merupakan bukti kehadiran seseorang pada satu kegiatan, daftar presensi kelas misalnya. Dengan kata lain, tanda tangan adalah bukti persetujuan seseorang yang valid dan formal yang kekuatannya dilindungi hukum. Pemberian tanda tangan oleh seseorang pasti bernilai valid dan diakui hukum, namun terkadang disalahgunakan, misalnya seperti pemalsuan tanda tangan untuk keuntungan pribadi atau suatu kelompok. Penyalahgunaan tersebut jelas melanggar hukum yang berlaku.

Pemberian tanda tangan yang sekarang digunakan adalah pemberian tanda tangan konvensional atau manual, yaitu dengan memberikan tanda tangan di atas kertas oleh orang yang berwenang memberikan tanda tangan. Penggunaan metode ini memiliki kelemahan dan kelebihan, kelebihannya adalah nilai orisinalitas dari tandan tangan dapat terjamin karena bertemu langsung dengan si pemberi tanda tangan, kekurangannya adalah ketika jumlah dokumen yang ditandatangani sangat banyak atau ketika si pemberi tanda tangan tidak sedang berada di tempat namun urgensi tanda tangan tersebut sangat tinggi.

Metode lain yang pernah penulis lihat adalah dengan menggunakan media digital, yaitu tanda tangan dengan media digital, tidak perlu si pemberi tanda tangan memberikan tanda tangannya ketika setempat dengan pemohon tanda tangan, cukup lewat media surat elektronik, Metode ini sangat praktis digunakan karena si pemohon tidak perlu bertemu dengan si pemberi tanda tangan, namun dengan mudahnya menyalin berkas di media digital maka otorisasi dan orisinalitas yang ada perlu dipertanyakan.

Pada makalah ini akan dipaparkan rancangan sistem pemberian tanda tangan dengan menggunakan media digital dengan memanfaatkan konsep tanda tangan digital pada ilmu kriptografi. Sistem ini diharapkan dapat meningkatkan kemudahan dalam pemberian tanda tangan melalui media digital tanpa mengurangi orisinalitas dari tanda tangan.

II. LATAR BELAKANG

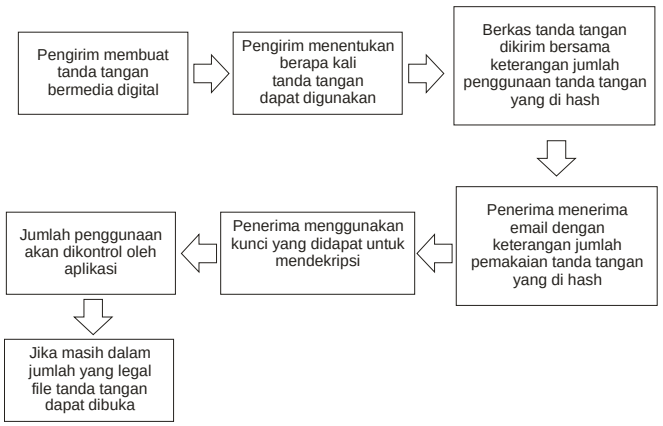
Penyebaran tanda tangan yang bisa dibilang menggunakan metode konvensional tergolong tidak praktis, karena si pemberi tanda tangan harus hadir dan berada setempat dengan si pemohon tanda tangan. Terlepas dari keunggulan metode tersebut dipercaya menjamin keamanan dan orisinalitas tanda tangan. Akan menjadi pelik ketika si pemohon membutuhkan tanda tangan dalam tenggat waktu yang terbatas namun si pemberi tanda tangan yang berwenang sedang tidak ada di tempat. Dengan menggunakan metode bermedia digital hal ini dapat diatasi, dengan menggunakan pengiriman surat elektronik dengan sisipan berupa tanda tangan yang telah discan, hal tersebut dapat diselesaikan. Namun tetap saja isu keamanan dan orisinalitas menjadi sulit dikontrol pada metode ini.

Dengan menggunakan pembatasan pada hak akses dan hak penggunaan tanda tangan tersebut, maka kedua masalah tersebut, yaitu masalah pada metode konvensional dan metode bermedia digital dapat diselesaikan. Sebenarnya kedua hal inilah yang mendasari penulis untuk memikirkan satu solusi yang dapat menyelesaikan kedua permasalahan utama tersebut.

III. SOLUSI YANG DITAWARKAN

Pada dasarnya, melihat kedua permasalahan tersebut, penulis menawarkan satu solusi berupa aplikasi yang mirip email client seperti yahoo, Mozilla thunderbird, Microsoft outlook, dan lain-lain, yang dapat mengirim file berupa gambar tanda tangan dari si pemberi tanda tangan yang dibatasi jumlah pemakaiannya oleh aplikasi sehingga si pemohon tidak dapat menggunakan tanda tangan tersebut seenaknya.

Konsep yang digunakan pada solusi yang ditawarkan ini adalah menggunakan konsep tanda tangan digital pada ilmu kriptografi. Dengan menggunakan konsep tersebut, akan dikirim bersama file tanda tangan, dan jumlah pemakaian tanda tangan (download atau buka berkas yang bersangkutan) yang diperbolehkan yang dihash menjadi sebuah message digest dengan menggunakan algoritma SHA-1. Untuk membuka berkas tanda tangan tersebut si penerima harus mengetahui nilai kunci n dan d dan dihitung satu kali pembukaan berkas. Misal si pemberi tanda tangan ingin memberikan otorisasi tanda tangan terhadap si A sebanyak 3 kali penggunaan, maka si A akan diberikan kunci n dan d yang hanya dapat digunakan 3 kali, setelah itu berkas tanda tangan yang dikirim tidak dapat digunakan lagi oleh si penerima tanda tangan.



Gambar 1 Proses yang terjadi dalam aplikasi

Pembatasan jumlah penggunaan tanda tangan adalah kunci dari sistem ini. Konsep tanda tangan digital dari kelimuan kriptografi akan digunakan untuk menghasilkan hash yang ikut dikirimkan ke penerima yang bersifat hidden, hanya aplikasi yang dapat membacanya, seperti header pada file HTML. Penerima hanya dapat membuka berkas ketika kunci yang dimasukkan sesuai.

IV. DASAR TEORI

SHA-1

Adalah salah satu algoritma hashing yang sering digunakan. Sebuah message akan di hash menggunakan algoritma ini lalu akan menghasilkan sebuah message digest yang terdiri dari 40 karakter heksadecimal.

Adapun pseudocode dari algoritma hashing ini adalah sebagai berikut :

```
h0 = 0x67452301
h1 = 0xEFCDAB89
h2 = 0x98BADCFE
h3 = 0x10325476
h4 = 0xC3D2E1F0

Pre-processing:
append the bit '1' to the message
append 0 ≤ k < 512 bits '0', so that
the resulting message length (in bits)
   is congruent to 448 ≡ −64 (mod 512)
append length of message (before pre-
processing), in bits, as 64-bit big-
endian integer

Process the message in successive 512-
bit chunks:
break message into 512-bit chunks
for each chunk
    break chunk into sixteen 32-bit
big-endian words w[i], 0 ≤ i ≤ 15

    Extend the sixteen 32-bit words
into eighty 32-bit words:
    for i from 16 to 79
        w[i] = (w[i-3] xor w[i-8] xor
w[i-14] xor w[i-16]) leftrotate 1

    Initialize hash value for this
chunk:
    a = h0
    b = h1
    c = h2
    d = h3
    e = h4

    Main loop:
    [25]
    for i from 0 to 79
        if 0 ≤ i ≤ 19 then
            f = (b and c) or ((not b)
and d)
            k = 0x5A827999
        else if 20 ≤ i ≤ 39
            f = b xor c xor d
            k = 0x6ED9EBA1
        else if 40 ≤ i ≤ 59
            f = (b and c) or (b and d)
or (c and d)
            k = 0x8F1BBCDC
        else if 60 ≤ i ≤ 79
            f = b xor c xor d
            k = 0xCA62C1D6

        temp = (a leftrotate 5) + f +
e + k + w[i]
        e = d
        d = c
        c = b leftrotate 30
        b = a
        a = temp
```

```
    Add this chunk's hash to result so
far:
    h0 = h0 + a
    h1 = h1 + b
    h2 = h2 + c
    h3 = h3 + d
    h4 = h4 + e

Produce the final hash value (big-
endian):
digest = hash = h0 append h1 append h2
append h3 append h4
```

dari Wikipedia.org

Penggunaan algoritma SHA-1 pada aplikasi distribusi tanda tangan tersebut adalah menghasilkan message digest dari jumlah penggunaan legal yang dikirmkan.

DIGITAL SIGNATURE

Adalah salah satu metode untuk memastikan bahwa pesan yang dikirim seseorang adalah valid dan belum berubah di pihak penerima. Pada makalah ini algoritma digital signature yang digunakan adalah RSA.

RSA

RSA adalah salah satu algoritma yang digunakan dalam implementasi tanda tangan digital. Adapun pembangkitannya adalah sebagai berikut :

1. Pilih dua bilangan prima $p \neq q$ secara acak dan terpisah untuk tiap-tiap p dan q. Hitung $N = p\ q$. N hasil perkalian dari p dikalikan dengan q.
2. Hitung $\varphi = (p\text{-}1)(q\text{-}1)$.
3. Pilih bilangan bulat (*integer*) antara satu dan φ ($1 < e < \varphi$) yang juga merupakan coprime dari φ.
4. Hitung d hingga $d\ e \equiv 1 \pmod{\varphi}$.

Setelah mendapatkan beberapa nilai kunci yang dibutuhkan untuk membuat tanda tangan digital, akan dilakukan enkripsi, yaitu dengan cara :

$$c = n^e \mod N$$

Sedangkan untuk melakukan dekripsi digunakan :

$$n = c^d \mod N$$

Penggunaan RSA sendiri adalah untuk mengirimkan jumlah otorisasi yang diberikan dan mendekripsinya pada sisi penerima untuk mendapatkan message digest awal dari pengirim. Message digest dari pengirim sendiri adalam jumlah penggunaan otorisasi yang digunakan. Setelah itu untuk mengetes apakah otorisasi masih bersifat legal, akan dilakukan counter terhadap message digest yang ada, apakah counternya masih di dalam batas yang diperbolehkan atau sudah melewati batas otorisasi yang diperbolehkan.

V. CARA KERJA SISTEM

Pada dasarnya, cara kerja sistem sama dengan cara kerja email client pada umumnya, hanya saja file yang dikirim adalah dibatasi pada file gambar, dan dalam pengirimannya akan disisipkan pesan terenkripsi dengan menggunakan algoritma yang telah dijelaskan sebelumnya, sehingga terjamin keamanannya. Pesan terenkripsi tersebut adalah jumlah berapa kali file tanda tangan tesebut dapat digunakan.

Saat file dikirim, pemberi tanda tangan akan memasukkan inputan berupa berapa kali file tanda tangan tersebut dapat digunakan oleh si penerima. Nominal tersebut akan di hash menggunakan aplikasi ini menjadi sebuah dan dikirim dengan sebelumnya dienkripsi dengan algoritma RSA.

Saat file diterima oleh aplikasi di sisi client, maka si penerima harus memasukkan nilai kunci yang benar yaitu nilai n dan d, untuk melakukan dekripsi. Dari hasil dekripsi tersebut, yang merupakan message digest dari nominal yang terkirim, akan dicocokkan dengan database hash berapakan nominal angka yang diperbolehkan. Setelah itu akan dilihat dari counter yang ada di dalam internal sistem untuk file ini telah digunakan berapa kali. Jika masih dalam kategori legal (masih dalam batas penggunaan) maka aplikasi tersebut akan mengijinkan menggunakan file tanda tangan tersebut. Jika tidak file tersebut tidak dapat disave ataupun diprintscreen ataupun digunakan.

Gambar 2 Proses enkripsi tanda tangan digital

Pada gambar di atas, tanda tangan digital akan dikirimkan juga pada file gambar yang akan dikirim.

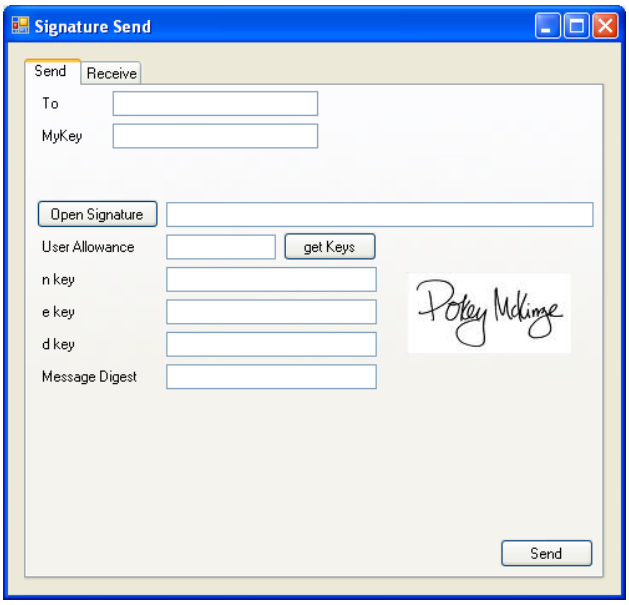
Gambar 3 Proses dekripsi tanda tangan digital

Pada gambar di atas, tanda tangan digital akan dicheck dulu sebelum penerima dapat membuka file, dan akan dibandingkan counter yang ada untuk file spesifik dengan jumlah otorisasi yang ada di message digest. Jika memang masih di dalam batas yang diperbolehkan dan kunci yang digunakan benar maka penerima dapat menggunakan file tanda tangan tersebut satu kali. Jika ingin menggunakan tanda tangan tersebut untuk kedua kalinya, maka pengguna harus memasukkan kembali kunci yang diterima. Counter akan terus bertambah ketika kunci dimasukkan.

VI. GAMBARAN SISTEM DAN ANTARMUKA

Sistem ini diimplementasikan ke dalam sebuah aplikasi desktop base yang kurang lebih sama seperti email client yang banyak ditemui. Namun diberi tambahan berupa “pengaman” berkas tanda tangan yang digunakan sehingga tidak dapat digunakan sembarangan.

Adapun pertama-tama antarmuka yang muncul adalah sebagai berikut :



Gambar 4 Antarmuka Send Signature

Antarmuka ini berfungsi untuk mengirim tanda tangan melalui suatu jaringan terdistribusi yang tidak dibahas pada makalah ini. Penjelasannya adalah sebagai berikut :

1. Label To

   Adalah alamat email tujuan si penerima, Email tersebut berbentuk khusus dan hanya dapat dibuka dengan aplikasi ini.

2. Label MyKey

   Adalah kunci unik untuk membedakan dokumen tanda tangan yang dikirim

3. Button Open Signature

   Membuka file tanda tangan bermedia digital yang telah dibuat sebelumnya, tidak terintegrasi dengan aplikasi ini.

4. Label User Allowance

   Adalah jumlah penggunaan yang diperbolehkan pada sisi penerima. Berbentuk bilangan bulat, selain bilangan bulat akan ada pesan kesalahan.

5. Button get Keys

   Melakukan generate key n, e, dan d, juga untuk menghasilkan message digest.

6. Label n key

   Adalah parameter n pada RSA yang digenerate.

7. Label e key

   Adalah parameter e pada RSA untuk enkripsi yang digenerate.

8. Label d key

   Adalah parameter d pada RSA untuk dekripsi yang digenerate.

9. Label Message Digest

   Hasil hashing berupa message digest

10. Image

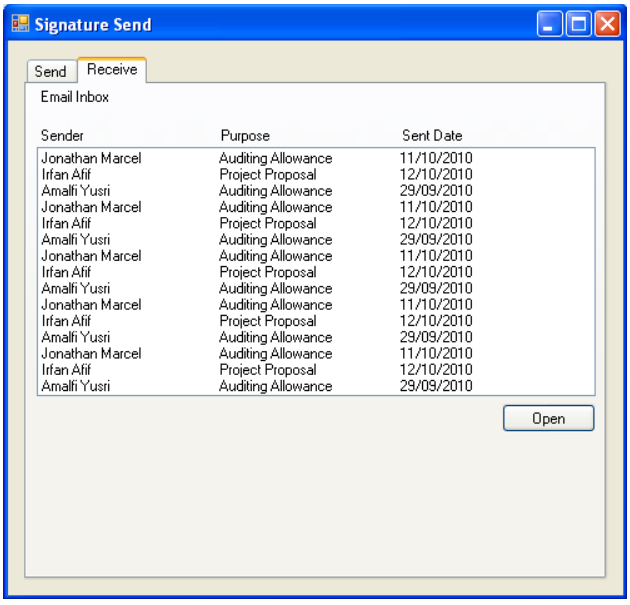
    Gambar image yang diopen sebelumnya pada button open Signature

11. Button Send

    Mengirim tanda tangan setelah semua field yang dibutuhkan terisi.

Setelah dikirm, email tersebut akan sampai ke inbox client / penerima dan dibuka dengan aplikasi ini juga.

Adapun antarmuka untuk sisi client yang juga terintegrasi dengan pengirim adalah sebagai berikut :



Sender	Purpose	Sent Date
Jonathan Marcel	Auditing Allowance	11/10/2010
Irfan Afif	Project Proposal	12/10/2010
Amalfi Yusri	Auditing Allowance	29/09/2010
Jonathan Marcel	Auditing Allowance	11/10/2010
Irfan Afif	Project Proposal	12/10/2010
Amalfi Yusri	Auditing Allowance	29/09/2010
Jonathan Marcel	Auditing Allowance	11/10/2010
Irfan Afif	Project Proposal	12/10/2010
Amalfi Yusri	Auditing Allowance	29/09/2010
Jonathan Marcel	Auditing Allowance	11/10/2010
Irfan Afif	Project Proposal	12/10/2010
Amalfi Yusri	Auditing Allowance	29/09/2010
Jonathan Marcel	Auditing Allowance	11/10/2010
Irfan Afif	Project Proposal	12/10/2010
Amalfi Yusri	Auditing Allowance	29/09/2010

Gambar 5 Antarmuka Receive Signature

Antarmuka ini berfungsi untuk memroses penerimaan email tanda tangan yang telah dikirim sebelumnya. Penjelasannya adalah sebagai berikut :

1. Listbox Sender PurposeSent Date

   User harus memilih email yang akan digunakan untuk diproses selanjutnya sesuai dengan purpose.

2. Button Open

   Membuka form dengan file yang bersesuaian untuk diproses selanjutnya.

Gambar 6 Antarmuka Unlock File

Pada antarmuka unlock file akan diberikan form kepada user untuk otorisasi. Penjelasan antarmukanya adalah sebagai berikut :

1. Label n key

   Penerima harus mengisi nilai n yang bersangkutan yang didapat dari si pengirim.

2. Label d key

   Penerima harus mengisi nilai derkipsi d yang bersangkutan yang didapat dari si pengirim.

3. Label MyKey

   MyKey adalah pengenal unik dari file tanda tangan yang bersangkutan.

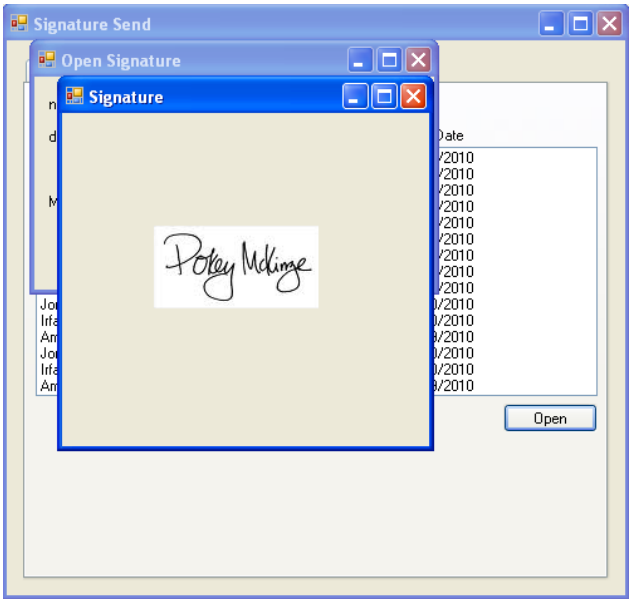
4. Button Submit

   Dengan menekan tombol ini, validasi inputan user akan dilakukan. Ketika valid dan masih berada dalam range otorisasi yang diperbolehkan maka akan muncul form selanjutnya, ketika tidak bisa maka tidak akan muncul form selanjutnya dan akan muncul pesan kesalahan.

5. Label Wrong key dst
   Pesan kesalahan yang muncul ketika nilai n dan d tidak sesuai atau range otorisasi telah melewati batasnya.

Antarmuka ini merupakan inti dari sistem aplikasi ini, ketika otorisasi berhasil akan muncul gambar tanda tangan yang dapat digunakan untuk suatu keperluan, ketika otorisasi gagal maka tanda tangan tidak dapat digunakan.

Antarmuka pengambilan tanda tangan adalah sebagai berikut :



Gambar 7 Pengambilan tanda tangan setelah berhasil otorisasi

VII. ANALISIS

Penggunaan aplikasi ini dapat membantu permasalahan ketidakhadiran pemberi tanda tangan yang berwenang ketika urgensi memaksa si pemohon tanda tangan untuk mendapatkan tanda tangan secara cepat. Pemberi tidak harus berada di tempat yang sama untuk memberika tanda tangannya kepada si penerima. Memberi tanda tangan akan semudah mengirim email ketika aplikasi ini berhasil diimplementasikan. Aplikasi ini jelas membantu jika implementasinya berhasil. Terlepas dari permasalahan koneksi internet tentunya.

Penggunaan SHA-1 sendiri sebenarnya adalah untuk melakukan hashing sehingga nilai jumlah otorisasi yang diberikan tidak plain terlihat ketika memang ditengah pengirimannya ada pihak yang tidak bertanggung jawab yang mencoba mengambilnya. Setelah dilakukan hashing, maka message digest yang telah dihasilkan sebelumnya akan di enkripsi menggunakan algoritma RSA. Sebenarnya penggunaan enkripsi RSA sendiri adalah untuk menambah keamanan dari nilai otorisasi yang dikirim. Ketika di dekripsi, nilai message digest akan dicocokkan dengan nilai yang ada di database untuk mengetahui berapa nilai bilangan bulatnya, setelah itu akan dicek sisa kemungkinan penggunaan yang diperbolehkan apakah tanda tangan masih dapat digunakan atau tidak, tentunya melihat kode MyKey yang digunakan.

Kelebihan aplikasi ini seperti yang telah disebutkan diatas adalah memudahkan penggunanya untuk mendapat tanda tangan pemberi tanda tangan walaupun si pemberi tidak berada di tempat. Selain itu pemberi tanda tangan tidak harus menandatangani dokumen yang jumlahnya sangat

banyak, hanya perlu menggunakan softcopy dokumen yang diprint.

Namun dibalik itu ada pula kekurangannya, yaitu ketika kita menggunakan prinsip sistem terdistribusi maka reliabilitas dari data akan berkurang, tingkat keamanan juga berkurang walaupun sudah ada mekanisme mengamankan orisinalitas data. Selain itu, aplikasi ini dibatasi oleh fitur jaringan, ketika jaringan menjadi suatu kendala maka aplikasi ini tidak bisa digunakan.

VIII. KESIMPULAN

Sistem ini sangat berguna ketika ideal diimplementasikan karena memudahkan pengguna dalam bertukan tanda tangan dan otorisasi pada suatu organisasi. Namun terlepas dari kelebihannya, aplikasi ini masih perlu banyak perbaikan terutama di bidang pengamanannya.

IX. PUSTAKA

http://en.wikipedia.org/wiki/SHA-1, diakses pada 15 Mei 2010, 20:20 WIB
http://id.wikipedia.org/wiki/RSA, diakses pada 15 Mei 2010, 20:21 WIB
http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/bahankuliah2006.htm, diakses pada 14 Mei 2010, 18:10 WIB

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, 16 Mei 2010

Amalfi Yusri Darusman, 13507023