Pengembangan Aplikasi Tanda Tangan Digital Sederhana dengan Protokol Khusus

Timotius Triputra Safei 13509017
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509017@std.stei.itb.ac.id

***Abstract*— Pengembangan aplikasi tanda tangan digital sudah banyak dilakukan. Penggunaan berbagai algoritma dan protocol sudah dilakukan dengan berbagai tujuan. Akan tetapi hal tersebut dilakukan sejalan dengan berbagai kerumitan untuk meningkatkan keamanan. Oleh karena itu, akan dikembangkan aplikasi sederhana yang diharapkan mampu digunakan di lingkungan kampus. Akan tetapi, aplikasi ini tidak hanya sederhana tetapi juga memiliki tingkan keamanan tinggi, serta beberapa keunggulan lainnya.**

Untuk mencapau hal tersebut, aplikasi ini akan memiliki mekanisme dan protocol khusus. Aplikasi ini mengambil informasi dari computer yang digunakan untuk memberikan tanda pembuat. Selain itu akan ada protocol khusus untuk meningkatkan kekuatan tandatangan digital. Contohnya adalah pengecekan author, penggunaan algoritma enkripsi dan proses validasi yang hanya bisa dilakukan di computer author. Lingkup permasalahan terbatas pada file dokumen.

***Index Terms*—*Protokol,Tanda tangan digital*.**

I. INTRODUCTION

Kriptografi adalah seni untuk menjaga keamanan data dan pesan yang kita miliki. Akan tetapi, kegunaan kriptografi bukan hanya pada hal tersebut. Dalam kriptografi ada beberapa aspek yang perlu dijaga.

Kriptografi memiliki beberapa tujuan yang perlu dicapai. Beberapa unsur tersebut adalah sebagai berikut:

1. *Data Confidentiality*

Salah satu aspek keamanan utama dari kriptografi tentu saja kerahasiaan dari pesan yang kita miliki. Dalam kriptografi, salaha satu tujuan utaqma adalah berusaha menjaga kerahasiaan pesan yang kita miliki. Pesan yang ada tidak boleh diketahui sembarang orang. Oleh karena itu, kerahasiaan pesan juga termasuk menjaga agar hanya orang yang diperbolehkan yang dapat melihat isi dari pesan tersebut.

2. *User Authentication*

Aspek ini berkaitan dengan siapa pengirim pesan tersebut. Pertanyaan utama dari aspek ini adalaha apakah pesan tersebut adalah pesan yang berasal pihak yang benar-benar mempunyai izin ataukan ada pihak lain yang sengaja mengirim pesan yang palsu.

3. *Message Authentication*

Dalam pengiriman pesan, sangat mungkin terjadi modifikasi pesan, baik secara tidak sengaja ataupun disengaja. Oleh karena itu, salah satu layanan kriptografi adalah bagaimana menjaga keaslian pesan yang kita kirim ataupun yang kita terima.

4. *Nonrepudiation*

Layanan lainnya dari kriptografi adalah anti penyangkalan. Dalam prosesnya kriptografi mengupayakan agar pesan yang dirubah tidak dapat disangkal oleh pengirimnya.

Untuk mencapai hal tersebut, banyak metode dan mekanisme yang dapat ditempuh. Sebagai contoh, dalam kriptografi dikenal metode enkripsi dekripsi. Metode ini digunakan untuk menyamarkan pesan yag dikirim menjadi pesan tidak bermakna sehingga dapat menjaga kerahasiaan pesan.

Metode untuk melakukan proses enkripsi dekripsi pun sangat beragam. Dalam kriptografi dikenal dua jenis metode enkripsi dekripsi. Yang pertama adalah metode simetrik dan asimetrik.

Metode enkripsi adalah proses penyembunyian pesan dengan menggunakan algoritma tertentu. Dalam kriptografi modern, yang menjadi kunci kekuatan algoritma tersebut bukanlah kerahasiaan algoritma. Akan tetapi, pada masa kini kekuatan kriptografi ditentukan dari kunci untuk melakukan enkripsi dekripsi. Untuk melakukan enkripsi dan kemudian mengembalikan pesan kembali seperti semula, diperlukan kunci yang menjadi parameter algoritma.

Kriptografi simetrik menggunakan hanya satu buah kunci untuk kedua proses enkripsi maupun dekripsi. Penggunaan kunci yang sama mempermudah proses dari segi pembangkitan kunci. Selain itu, kunci simetri biasanya berukuran kecil dan dapat diingat. Akan tetapi, penggunaan kunci simetrik ini mempunyai beberapa kelemahan.

Selain itu, terdapat juga kriptografi asimetrik, yaitu kriptografi dengan menggunakan dua buah kunci yang berbeda untuk enkripsi dan dekripsi. Kriptografi ini cukup

kuat apabila memenuhu persyaratan yaitu kunci yang panjang. Akan tetapi hal tersebut memunculkan kelemahan yaitu lambatnya komputasi proses.

Selain enkripsi dekripsi, maka terdapat juga metode tanda tangan digital. Metode ini dapat menyelesaikan masalah no 2-4 dari 4 aspek dalam kriptografi.

II. TANDA TANGAN DIGITAL

Tanda tangan adalah suatu mekanisme yang digunakan untuk menandai suatu dokumen. Lewat tanda tangan, orang mengakui beberapa hal terhadap dokumen tersebut. Pengakuan tersebut mungkin saja dalam bentuk persetujuan atau kepemilikan. Contohnya, orang yang menandatangani suatu dokumen mengakui bahwa ia menyetujui isi dokumen. Selain itu, mungkin saja penandatanganan dokumen menandakan bahwa orang tersebut mengakui bahawa dokumen tersebut adalah miliknya.

Pada masa kini, dokumen yang digunakan tidak hanya berupa dokumen tertulis yang dapat langsung dibubuhi tanda tangan. Oleh karena itu, dibutuhkan suatu mekanisme tanda tangan untuk memberikan tanda tangan keapda dokumen dalam bentuk digital. Mekanisme yang dimaksud bukannlah memberikan hasil scan atau masukan dari user dalam bentuk tanda tangan, tetapi suatu mekanisme algoritma kriptografi yang menghasilkan tanda tangan sesuai dengan isi pesan dan pengirim.

Tanda tangan memiliki beberapa sifat yang harus diperhatikan, yaitu

1. Tanda tangan sebagai bukti otentik
2. Tanda tangan dapat dilupakan
3. Tanda tangan tidak boleh digunakan ulang untuk dokumen lain
4. Deokumen yang sudah diberi tanda tangan, tidak boleh dirubah
5. Tanda tangan tidak dapat disangkal.

Penandatanganan dapat dilakukan dengan beberapa cara. Contoh penandatanganan pesan adalah dengan menggunakan fungsi Hash dan algoritma enkripsi.

A. Algoritma Enkripsi

Penggunaan algoritma enkripsi kunci simetri dianggap sudah memberikan tanda digital karena hasil enkripsi sudah tergantung dari pesan dan pengirim. Selain itu, enskripsi hanya bisa dilakukan oleh pihak yang mengetahui kunci, dalam hal ini pengirim dan penerima.

Apabila satu pihak mengirim hasil enkripsi kepada pihak kedua, maka pihak kedua dapat memastikan dari pesan tersebut bahwa pihak pertamalah yang mengirim pesan karena kunci algoritma hanya diketahui kedua pihak. Hal ini dapat mmenyelesaikan permasalahan kriptografi mengenai otentikasi pengirim dan juga keaslian pesan. Bahkan sebenarnya menyelesaikan masalah nomor 1.

Akan tetapi, metode ini mempunyai kelemahan yaitu tidak dapat menyelesaikan permasalah nomor 4. Mekanisme ini tidak memberikan solusi untuk permasalah penyangkalan. Apabila pihak pertama menyangkal bahawa ia mengirim pesan atau mmenyangkal isi dari pesan tersebut.

Salah satu metode untuk menyelesaikan masalah ini adalah dengan menggunakan pihak ketiga. Pihak ketiga mengetahui kunci pihak pertama dan pihak kedua, akan tetapi kedua pihak tersebut tidak mengetahui kunci dari pihak lainnya.

Apabila salah satu pihak ingin mengirim pesan maka pihak tersebut mengirim pesan yang sudah dienkripsi dengan kunci miliknya ke pihak ketiga. Oleh pihak ketiga, pesan didekripsi menggunakan kunci pengirim, memberikan pernyataan pesan benar-benar dikirim oleh pengirim, mengenkripsi pesan dengan kunci penerima dan kemudian mengirim pesan baru ke penerima.

Dengan metode ini, pengirim tidak dapat menyangkal pesan yang diterima penerima karena pernyataan dari pihak ketiga dapat membuktikan bahwa benar pihak pertama yang mengirimkan pesan. Selain itu pihak ketiga dapat memastikan bahwa pesan dikirim dari pihak pertama karena hanya kedua pihak tersebut yang mengetahui kunci pihak pertama.

Akan tetapi metode ini memiliki prasyarat. Prasyarat pertama adalah adanya pihak ketiga yang dapat dipercaya. Selain itu, kunci algoritma harus dimiliki hanya oleh pihak ketiga san pihak yang memiliki kunci. Apabila kunci ini bocor keluar, maka metode ini tidak dapat digunakan. Selain itu, jika menggunakan metode ini maka pihak ketiga dapat mengetahui isi dari pesan yang dikirim.

Selain penggunaan algoritma simetrik, dapat digunakan juga algoritma kunci asimetrik. Ide untuk penggunaan ini ditemukan oleh Diffie dan Hellman. Ide utama dari cara ini adalah menggunakan kunci privat untuk mengenkripsi pesan dan menggunaka kunci public untuk mendekripsi pesan. Metode ini menyelesaikan semua aspek kriptografi, tetapi tidak dengan sempurna.

Algoritma yang mendukung hal ini adalah algoritma yang bersifat $D_{SK}(E_{PK}(M)) = M$ dan $D_{PK}(E_{SK}(M)) = M$. Contoh algoritma yang memenuhi hal ini adalah RSA.Pesan yang dikirim dienkripsi terlebih dahulu baru kemudian si penerima mendekripsi menggunakan kunci public. Akan tetapi, ketidaksempurnaan dari metode ini terdapat pada aspek kerahasiaan pesan. Kerahasiaan pesan tidak terjamin seutuhnya karena kemungkinan kunci public dimiliki tidak hanya oleh pihak penerima, tetapi oleh pihak lainnya.

B. Fungsi Hash

Cara penandatanganan lainnya adalah menggunakan fungsi hash. Apabila penggunaan algoritma enkripsi dapat menyelesaikan semua aspek kriptografi, maka penggunaan fungsi hash hanya dapat menyelesaikan permasalahan otentikasi pesan yaitu aspek ke 2-4. Hal ini dapat digunakan karena terkadang kita hanya membutuhkan penyelesaian masalah otentikasi pesan tanpa perlu

merahasiakan isi pesan tersebut seperti masalah tanda tangan pada dokumen tertulis.

Penggunaan fungsi has biasanya bersamaan dengan penggunaan kunci asimetrik karena dapat menyelsaikan masalah *non-repudiation*.

Cara penggunaan fungsi hash adalah membuat *message digest* dari pesan yang dikirim. MD yang dihasilkan pasti berbeda untuk setiap pesan sesuai dengan sifat fungsi hash. Selain itu, dari MD tidak dapat ditemukan pesan aslinya. Oleh karena itu, tanda tangan menggunakan fungsi hash dapat menjamin setiap tanda tangan hanya digunakan 1 kali untuk 1 pesan dan tidak dapat digunakan ulang.

Setelah didapatka MD, maka MD tersebut dienkripsi menggunakan kunci privat dari pengirim. Setelah itu, pesan yang sudah ditambahkan dengan tanda tangan dikirim kepada penerima.

Penerima dapat memastikan keabsahan pesan lewat proses verivikasi. Pertama-tama penerima membuat MD dengan menggunakan fungsi hash yang sama dengan pengirim. Selain itu, penerima juga mendekripsi tanda tangan digital yang diterima bersamaan dengan pesan. Setelah itu bandingkan kedua MD.

Keabsahan pesan dapat dilihat dari hasil perbandingan MD yang didapat. Apabila MD yang dibuat sendiri sama dengan MD yang didapat dari proses dekripsi, maka pesan dapat dijamin keabsahannya.

Algoritma yang sering digunakan adalah RSA dan ElGamal. Pada algoritma RSA, proses enkripsi dan dekripsi merupakan proses yang identic, oleh karena itu, proses penandatangan maupun verifikasi identic.

III. ALGORITMA YANG DIGUNAKAN

A. Digital Signature Algorithm

Salah satu algoritma yang digunakan adalah DSA. DSA adalah algoritma hasil dari pengembangan algoritma ElGamal. Algoritma ini merupakan algoritma asimetrik yang menggunakan 2 kunci yaitu kunci public dan kunci privat.

Bentuk parameter dan kunci dari algoritma ini adalah

p = bilangan prima dengan panjang bit 512 <= p <= 1024 dengan panjang p kelipatan 64.
q = bilangan prima 160 bit dan memenuhi sifat (p-1) mod q = 0.
$g = h^{(p-1)/q}$ mod p dengan h < p -1
x = bilangan bulat lebih kecil dari q
$y = g^x$ mod p
m = pesan

Dari parameter tersebut, dibentuk kunci privat maupun public sebagai berikut:

kunci public = (p,q,g,y)
kunci privat = (p,q,g,x)

Tanda tangan terdiri dari 2 bagian r dan s. Penandatanganan menggunakan message digest dari m. MD dihasilkan lewat fungsi hasn H. berikut ini cara perhitunnngan tanda tangan

$r = (g^k \bmod p) \bmod q;$
$s = (k^{-1} (H(m) + x * r)) \bmod q$

Proses verifikasi dilakukan dengan cara membandingkan r dan hasil perhitungan yang didapat. Berikut in perhitungannya

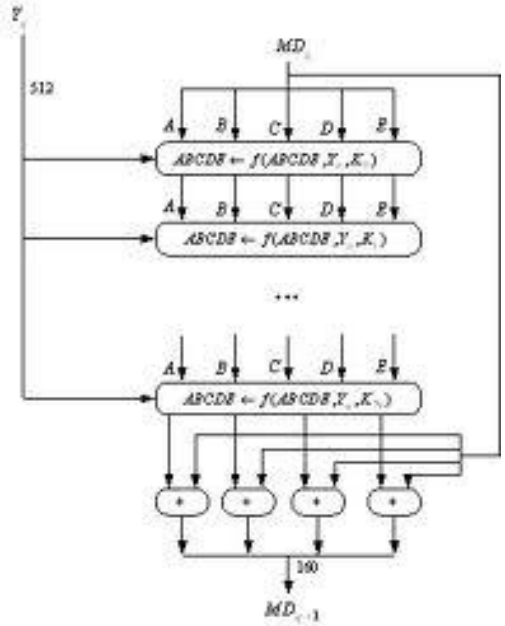
$w = s^{-1} \bmod q$
$u_1 = (H(m) * w)$ moq q
$u_2 = (r*w) \bmod q$
$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q)$

Apabila v dan r sama, maka tanda tanga tersebut sah.

B. SHA

SHA adalah salah satu algoritma fungsi hash yang sering digunakan. Fungsi in dibuat dari NIST. Fungsi ini merupakan fungsi satu arah, yang dijadikan standard oleh NSA.

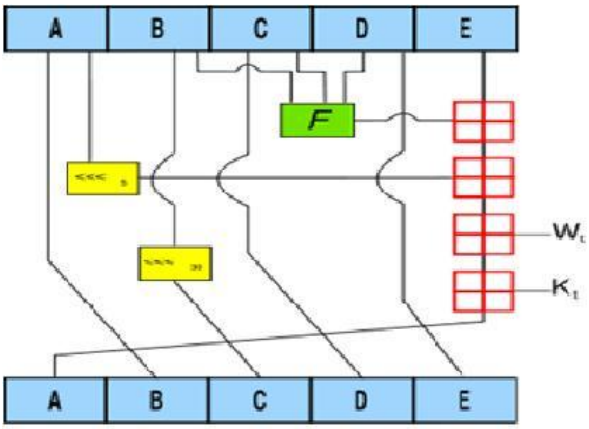
Fungsi ini mengolah pesan dengan panjang masksimum 2^{64} bit. Dari fungsi ini akan dihasilkan MD sepanjang 160 bit. Pesan akan diberi bit pengganjal sehingga panjang pesan kongruen dengan 448 mod 512 atau kurang 64 bit dari kelipatan 512. Panjang bit pengganjal adalah 1 – 512 bit karena pesan 448 bit tetap ditambah bit pengganjal. Nbit pengganjal adalah bit 1 dikuti sisanya 0. Berikut ini proses dasar SHA.



Terdapat 5 buah buffer yaitu A,B,C,D,E dengan panjang masing-masing 32 bit. Kelima penyangga diinisialisasi sebagai berikut (dalam hex)

A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
E = C3D2E1F0

Proses SHA terdiri dai 80 putaran dari proses di bawah ini



a,b,c,d,e = buffer 32 bit
t = putaran (0 - 79)
f_t = fungsi logika
$<<<_s$ = circular left shift sebanyak s
W_t = word 32 bit dari 512 bit yang diproses dengan W_1 – W_{16} adalah word yang diproses dan sisanya
$W_t = W_{t-16}$ XOR W_{t-14} XOR W_{t-8} XOR W_{t-3}
K_t = kontanta penambah
K 0 – 19 = 5A827999
K 20 – 39 = 6ED9EBA1
K 40 – 59 = 8F1BBCDC
K 60 – 79 = CA62C1D6

Putaran	$Fungsi_t$
0 - 19	(b∧c)∨(~b∧d)
20 – 39	b + c + d
40 – 59	(b∧c) ∨ (b∧d) ∨ (c∧d)
60 – 79	b + c + d

Setelah putaran ke 79, maka a,b,c,d,e ditambahkan kembali dengan A,B,C,D,E dan selanjutnya algoritma memproses blok data berikutnya (Y). Hasil akhirnya adalah gabungan dari bit-bit pada a,b,c,d,e.

IV. TUJUAN DAN DASAR PENGEMBANGAN

Aplikasi yang akan dibangun akan memiliki beberapa aturan khusu atau protocol yang diharapkan dapat memenuhi beberapa tujuan. Adapun fungsi tandatangan dari aplikasi ini adalah

1. Tanda tangan dapat menunjukkan bahwa dokumen yang ditandatangani sudah berubah (mengalami modifikasi) (message authentication)
2. Tanda tangan dapat menunjukkan apakah pesan yang dikirm benar-benar ditulis oleh pengirim (user authentication)
3. Penandatangan tidak dapat menyangkal bahwa ia yang mnandatangani pesan (*non-repudiation*)
4. Penandatangan dapat menunjukkan bahwa dokumen tersebut adalah miliknya meskipun sudah dirubah atau sudah dimodifikasi (*reclaim).*

Pembuatan protocol aplikasi ini didasari oleh keadaan yang ada di lingkungan kampus. Dari lingkungan tersebut, ada beberapa hal yang ingin dicapai.

Sebagai salah satu hal yang ingi dicapai adalah pencegahan plagiarisme. Pada pengembangan aplikasi ini ditambahkan aturan khusus untuk mencegah proses plagiat yang sering terjadi di lingkungan kampus. Pada lingkungan kampus erring terjadi pemakaina dokumen milik orang lain yang dirubah isinya. Oleh karena itu, aplikasi diharapkan mampu menunjukkan siapa yang membuat dokumen. Hal ini berlaku untuk dokumen yang sudah dirubah isinya (mengalami modifikasi).

Dengan aplikasi ini pemilik dapat menunjukkan bahwa ialah yang membuat dokumen tersebut meskipun sudah adap erubahan isi dokumen. Hal ini tidak bisa didapatkan dengan penandatanganan biasa.

Selain itu penggunaan kunci privat dan public yang disederhanakan untuk mempermudah penggunaan aplikasi. Hal ini didasari oleh pengguna aplikasi yang dituju adalah mahasiswa dan linggkup penggunaannya tidak secara global.

Selain itu, aplikasi ini dapat memenuhi tujuan dasar tanda tangan digital.

V. RANCANGAN PROTOKOL DAN APLIKASI

Dalam aplikasi in terdapat aturan atau protocol yang digunakan untuk membangun aplikasi. Berikut adalah rancangan aplikasi yang akan dibangun beserta aturan yang digunakan

1. Tanda tangan merupakan 2 bagian yang gabungkan.
2. Tanda tangan digabung dalam file, tetapi tidak tertulis di dalam dokumen. Tanda tangan diletakkan setelah EOP.
3. Cara penyimpanan file yang ditandatangani adalah *replace.* Jadi, jika file ditandatangani dan disimpan maka file asli akan terhapus.
4. Tanda tangan bagian pertama adalah *message digest* dari gabungan *MAC Address (Media Access Control)* dan *username* dari account yang digunakan di computer tempat proses berlangsung.
5. Fungsi hash yang digunakan adalah algoritma SHA dengan panjang MD 160 bit.
6. bagian kedua dari tanda tangan adalah hasil tanda tangan digital menggunakan *Digital Signature Standard* (DSS).
7. Algoritma yang digunakan adalah *Digital Signature Algorithm (DSA)* dan SHA.
8. Kunci privat yang digunakan adalah *MAC Address (Media Access Control)* dari computer yang digunakan. Setelah dibangkitkan kunci privat akan disimpan.
9. Kunci public yang digunakan akan dibangkitkan secara acak menggunakan seed dari kunci privat. Setelah dibangkitkan kunci public akan disimpan.
10. Dokumen yang sudah ditanda tangani, dapat ditanda

tangani ulang apabila ada perubahan isi hanya apabila bagian pertama sesuai.

11. Penghapusan tanda tangan dapat dilakukan hanya apabila bagai pertama sesuai.

12. Aplikasi menyediakan layanan verifikasi pengirim dengan masukkan kunci public.

13. Aplikasi menyediakan layanan *RECLAIM* yaitu menunjukkan bahwa dokumen tersebut ditandatangani di computer yang digunakan untuk menjalankan aplikasi.

14. Hasil dari RECLAIM ada 3 yaitu :

a. dokumen ditandatangani di computer tersebut dan isi dokumen tidak berubah

b. dokumen ditandatangani di computer tersebut tetapi isinya sudah berubah

c. proses RECLAIM gagal karena bagain pertama tidak sesuai ataupun tidak ada tanda tangan.

15. Pada proses RECLAIM, kunci akan dibangkitkan ulang.

16. Semua MAC Address didapatkan langsung dari system. Aplikasi tidak dapat menerima MAC Address dari user.

VI. ANALISIS

Rancangan aplikasi dan aturannya dibuat agar fungi serta tujuan dapat dicapai. Oleh karena itu, berikut ini analisi ketercapaian tujuan dan pemenuhan fungsi dasar dari tanda tangan digital.

Pada saat verifikasi, perubahan isi dokumen dapat dideteksi dari tanda tangan bagian kedua. Akan tetapi, ada beberapa keadaan yang mungkin terjadi.

Pertama, proses verifikasi pada computer pemberi tanda tangan (computer utama) dapat menggunakan kunci public atau pun kunci privat. Pada computer lain, maka diperlukan kunci public. Akan tetapi,, pada computer utama dapat digunakan fungsi RECLAIM untuk mengecek perubahan isi dokumen.

Selain untuk pengecekan perubahan isi, proses verifikasi juga dapat digunakan untuk memastikan siapa apakah pesan yag dikirim benar-bnar berasal dari pengirim yang diharapkan. Tentu saja hal ini membutuhkan kunci public.

Penggunaan DSS juga dapat memungkinkan untuk apliakasi memenuhi aspek *non-repudiation*. Karena dengan kuncli public tersebut, maka hanya pengirim yang dapat memberikan tanda tangan. Bahkan hal ini juga dapat dicapai dengan melakukan RECLAIM dari computer pengirim.

Akan tetapi hal ini dapat dilakukan jika username yang digunakan sama. Akan tetapi, sesuai dengan keadaan lingkungan penggunaan (kampus), diasumsikan bahwa computer utama yang digunakan mewakili pengirim. Hal ini dilihat dari hampir semua computer digunakna hanya oleh pemilik dan user biasanya hany amemiliki satu computer dengan satu account. Melihat hal tersebut, maka aplikasi ini kurang sesuai untuk lingkungan dengan pemakaian computer bersama.

Sebagai fungsi tambahan, layanan RECLAIM digunakan untuk mencapai berbagai tujuan lainnya. Layanan ini dapat digunakan untuk menunjukkan siapa penulis pesan. Hal ini dapat dilakukan dengan mencoba melakukan RECLAIM di computer user. Dari hasil tersebut, dapat dilihat apakah user tersebut adalah pemberi tanda tangan atau bukan.

Layanan ini juga dapat digunakan untuk menunjukkan bahwa suatu dokumen adalah milik seseorang. Seseorang yang ingin mengakui bahwa hal dokumen tersebut adalah miliknya dapat melakukan RECLAIM dari computer miliknya yang merupakan computer utama. Dari hal tersebut maka dapat ditentukan apakah benar bahwa ia yang menulis dokumen tersebut.

Hal ini dapat berguna untuk melawan plagiarism. Pihak yang merasa ditiru dapat menuntut dkepemilikan dokumen lewat layanan ini. Apalagi pada lingkunag kampus mungkin terjadi adalah dokumen asli yang masih memiliki tanda tangan, dirubah isinya agar seidkit berbeda. Tentu saja apabila dokumen di-plagiat dengan cara membuat baru atau tanda tangan dihapus secara paksa, maka proses RECLAIM gagal.

Akan tetapi, aplikasi ini mempunyai aturan sedemikian hingga mengurangi resiko plagiarism. Aturan tersebut adalah proses peghapusan tanda tangan yang hanya dapat dilakukan di computer utama. Hal ini mencegah agar tanda tangan tidak dapat dihapus sembarangan. Tanda tangan hanya dapat dihapus secara paksa lewat aplikasi lain. Hal ini hanya dapat dicegah apabila dokumen yang ada dilindungi atau bersifat *protected*.

Aturan lainnya adalah bentuk penyimpanan yang berupa *replace*. Hal in mencegah bocornya dokumen asli yang belum ditandatangani. Apabila dokumen asli dimiliki orang lain, maka orang lain bahkan dapat menandatangani dokumen tersebut dan mengaku bahwa dokumen tersebut adalah miliknya. Bahkan malah mungkin terjadi pemilik dokumen aslilah yang dianggap meniru atau mencuri isi dokumen.

Penggunaan MAC Address didasari bahwa MAC Address bersifat unik untuk setiap computer. Diharapkan dari analisa lingkungan yaitu computer yang digunakan bukanlah computer yang dipakai bersama, MAC Address dapat mewakili tiap computer secara unik. Dan tentu saja diasumsikan bahwa pemilik tiap computer unik.

Pemakaian MAC Address untuk pembangkitan kunci diharapkan dapat membuat aplikasi ini sederhana. User tidak perlu mebuat kunci sendiri. Bahkan apabila penggunaan aplikasi hanya sekedar untuk menandakan kepemilikan computer, kunci yang ada tidak perlu disimpan.

Hal tersebut dapat dilakukan apabila memang fungsi otentikasi user tidak diperlukan. Proses otentikasi pesan dapat dilakukan lewat RECLAIM di computer utama.

Pembangkitan kunci mengguanakan MAC Address juga dilihat dari lingkungan penggunaan. Karen penggunaan di kampus, maka panjang kunci yang dibutuhkan tidak

terlalu panjang. Pada lingkungan kampus, tingkat serangan yang mungkin terjadi tidak setinggi pada penggunaan global. Selain itu, kunci dapat dibangkitkan tanpa perlu mendaftarkan dan memiliki sertifikat.

Akan tetapi, tetap saja aplikasi ini memiliki kekurangan. Salah satu kekurangannya adalah proses yang cukup berat karena penggunaan DSS. Selain itu, pembangkitan kunci diperkirakan akan memakan waktu karena kunci yang dibangkitkan memiliki syarat tertentu.

Selain itu, aplikasi ini juga lemah terhadap serangan dari luar secara langsung. Tidak seperti watermark, aplikasi ini mnempatkan tanda tangannya di tempat khusus. Hal ini menyebabkan tanda tangam masih mungkin dihapus secara paksa.

Aplikasi ini juga memiliki batasan sendiri. Layanan RECLAIM hanya bisa dijalankan dari computer utama. Kita tidak dapat melihat langsung siapa penulis dokumen dari tempat lain. Hal ini dikarenakan semua MAC Address didapatkan secara langsung dari sistem. Hal tersebut untukk emningkatkan keamanan tanda tangan. Dari hal ini, diharapkan hanya tiap tanda tangan menunjukkan computer mana yang merupakan kumputer utama dan mencegah user menandatangani dokemen atas nama orang lain (menggunakan MAC Address orang lain).

VII. CONCLUSION

Aplikasi ini dapat digunakan untuk berbagai macam fungsi dan tujuan yang sudah disebutkan. .Fungsi yang dimaksudkan tentu saja mencakup fungsi dasar dari tanda tangan digital.

Aplikasi ini masih memiliki bebearapa kekurangan, oleh karena itu. Oleh karena itu, masih ada aspek danbagian dari aplikasi yang dapat dikembangkan lebih lanjut.

Aplikasi ini juga mempunyai batasan sendiri. Beberapa batasan diantaranya adalah lingkungan pemakaian dan user pemakai. Aplikasi ini kurang cocok dipakai di lingkup global, hanya cocok di lingkungan kecil seperti kampus. User merupakan pemakai computer pribadi. Aplikasi in tidak dianjurkan untuk computer dengan pemakian bersama.

REFERENCES

[1] Munir, Rinaldi, "Diktat Kuliah IF5054 KRIPTOGRAFI", Bandung : Departemen Teknik Informatika ITB, 2005.

[2] http://laksmana02.wordpress.com/

[3] http://top-bing.blogspot.com/2009/11/sha-1-algorithm.html

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, 14 Mei 20112

Timotius T. Safei