IMPLEMENTASI SECURITY SISTEM BERBASIS PROTOKOL S/MIME UNTUK PENGELOLAAN E-MAIL SEBAGAI UPAYA PENINGKATAN JAMINAN KEAMANAN DALAM TRANSAKSI INFORMASI SECARA ONLINE STUDI KASUS PT. BUANA JAYA

Sevi Andriasari[1]
Program Manajemen Informatika[1]
AMIK Lampung
Jl. ZA.Pagar Alam No. 17A Rajabasa Bandar Lampung
Email : andriasari.sevi@yahoo.com[1]

Abstract

Impact of information technology development in all aspects of human life, the way people communicate is beginning to be conventional to digital. E-mail is a service provided by information technology systems as a means to transact information in the digital world. Communicate using e-mail has many advantages, but on the other side of the attacker vulnerable to digital activity, such as wiretapping. Security is key to securing the information carried by e-mail. PT. Buana Jaya is an organization engaged in the business who handles the IT infrastructure among government and private agencies, which are traded daily confidential information using e-mail online. S/MIME is one alternative that safeguards can be implemented in the e-mail. The end result of this research in the form of a draft protocol implementation S/MIME at the e-mail of PT. Buana Jaya which applying cryptographic techniques such as digital signature and/or encryption are proven to meet the information security aspects. By implementing S/MIME, aspects of the information security such as confidentiality, integrity, authentication and non-repudiation are expected by PT. Buana Jaya can be met.

Keywords: e-mail, digital attackers, security, S/MIME, information security.

A. PENDAHULUAN

1. Latar Belakang Masalah

Perkembangan komunikasi digital semakin pesat setelah munculnya internet. Internet memberikan banyak layanan yang memungkinkan manusia saling bertukar informasi tanpa mengenal jarak dan waktu. Pengguna internet di seluruh dunia sampai dengan akhir tahun 2011 seperti yang tercatat dalam survey Internet World Stats pada internetworldstats.com mencapai 2.267.233.742 pengguna, dengan statistik tertinggi pengguna dari Asia mencapai 44,8% [IWS 2011].

Salah satu fasilitas internet yang paling banyak digunakan di dunia khususnya di Indonesia adalah e-mail *online*, karena dengan adanya e-mail para pengguna dapat saling bertukar informasi. Bahkan

tercatat dari hasil riset Ipsos bahwa 9 dari 10 (91%) pengguna internet di Indonesia menggunakan e-mail *online* untuk kirim/terima (transaksi) informasi [IPSOS 2012].

2. **Perumusan Masalah**

Berdasarkan latar belakang masalah yang telah diuraikan sebelumya, maka rumusan masalah dalam penelitian ini adalah :

1. Solusi apakah yang dapat diterapkan untuk menjamin kemanan transaksi informasi berbasis layanan e-mail *online* bagi PT. Buana Jaya?
2. Bagaimanakah rancangan implementasi protocol S/MIME pada layanan e-mail bagi PT. Buana Jaya?
3. Bagaimanakah perbandingan keamanan dari hasil simulasi sebelum dan sesudah implementasi rancangan tersebut?

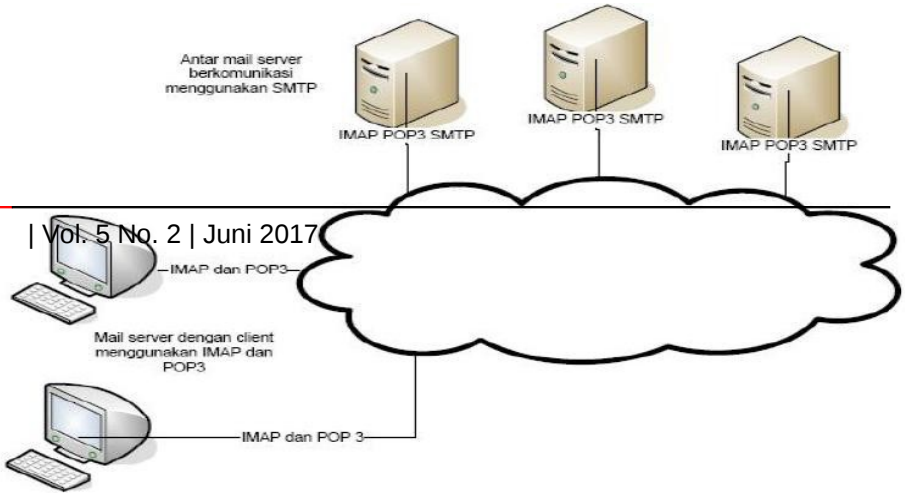
B. LANDASAN TEORI

1. E-mail

Elektronic mail atau dapat disebut dengan e-mail, merupakan salah satu layanan internet yang sangat popular dan paling banyak digunakan oleh berbagai kalangan, baik di lingkungan organisasi maupun perusahaan. E-mail digunakan untuk saling bertukar informasi atau mengirim pesan antara seseorang dengan orang lainnya yang terpisahkan oleh jarak dan kondisi cuaca apapun dengan melewati perangkat telekomunikasi.

Pengiriman e-mail tidak menggunakan kertas melainkan menggunakan suatu aplikasi berbentuk program komputer, dengan media komunikasi jaringan. E-mail memungkinkan seseorang menuliskan beberapa teks, mengidentifikasi pihak yang ingin dikirimi pesan dengan menuliskan alamat e-mail seseorang di bagian atas dan dikirimkan ke alamat tersebut. Dengan mengirimkan e-mail, seseorang dapat mengerjakan hal yang sama seperti mengirimkan e-mail kepada layanan pos. Layanan ini mengirim e-mail dan kemudian orang yang dikirim pesan memeriksa e-mailnya, kemudian menerima pesan yang telah orang lain kirimkan.

Tiap e-mail mencakup teks yang seseorang tuliskan dan alamat e-mail seseorang. E-mail memungkinkan seseorang untuk mengirim pesan ke banyak penerima sekaligus mengirim file menggunakan e-mail daripada menggunakan program transfer file. Rata-rata pesan dalam e-mail tidak mencapai sepuluh *kilobyte* dan beberapa pesan mengandung beberapa *megabyte* data, karena digunakan untuk mengirim file.



Gambar 1. Arsitektur Protocol pada e-mail [Nov 2009]

E-mail menggunakan suatu aplikasi berbentuk program komputer sebagai medianya. E-mail selalu memanfaatkan standar TCP/IP yaitu menggunakan IMF (*Internet Message Format*) untuk menentukan header yang digunakan untuk mengenkapsulasi teks e-mail, termasuk pengiriman e-mail dengan SMTP (*Simple Mail Transport Protocol*)/IMAP (*Internet Mail Access Protocol*) karena untuk mendapatkan pesan, maka akun e-mail sebelumnya harus terdaftarkan dulu di *mail server* yang akan dikontak. Kemudian menentukan terlebih dahulu protokol bagi klien untuk mendapatkan e-mail dari server yang dihubungi.

2. **Aspek Keamanan Jaringan Komputer**

Keamanan jaringan komputer melingkupi empat aspek utama yaitu *privacy/confidentiality*, *integrity*, *authentication* dan *availability* serta dua aspek lain yang erat kaitannya dengan keamanan komputer yang berbasis jaringan yaitu *access control* dan *non-repudiation*.

1. *Privacy/Confidentiality*

Aspek *privacy* merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses suatu sistem, dan lebih ke arah data-data yang sifatnya privat sedangkan *confidentiality* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu misalnya sebagai bagian dari pendaftaran sebuah layanan dan hanya diperbolehkan untuk keperluan tertentu tersebut.

2. *Integrity*

Integrity lebih menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi, adanya virus, *trojan*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang sering dihadapi, sebagai contoh misalnya sebuah e-mail dapat saja ditangkap di tengah jalan yang kemudian dimodifikasi dan diteruskan ke alamat yang dituju dengan kata lain keutuhan dari informasi tersebut sudah

tidak terjaga lagi, penggunaan enkripsi dan tanda tangan digital misalnya dapat mengurangi atau bahkan bisa menjadi salah satu solusi untuk mengatasi masalah tersebut.

3. *Authentication*
   Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, orang yang mengakses atau memberikan informasi adalah orang yang dimaksud atau server yang kita hubungi adalah server yang asli. Masalah pertama yang muncul membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan tanda tangan digital, masalah selanjutnya biasanya berhubungan dengan *access control* yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi dalam hal ini pengguna harus menunjukkan bukti bahwa memang dirinya adalah pengguna yang sah, misalnya dengan menggunakan *password* atau cirri-ciri khusus yang berhubungan dengan pemilik/pengguna yang sah seperti PIN, sidik jari, biometric dan lain-lain.
4. *Availability*
   Availability berhubungan dengan ketersediaan informasi ketika dibutuhkan, sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi salah satu contohnya adalah serangan Dos (*Denial Of Service*) dimana server biasanya dengan mengirim *request* yang berkelanjutan atau permintaan di luar perkiraan sehingga tidak dapat melayani permintaan lain atau behkan sampai *down*, *hang* atau *crash*.
5. *Access Control*
   Access control berhubungan dengan cara pengaturan akses kepada informasi dan biasanya berhubungan dengan klasifikasi data (publik, privat, *confidential*, *top secret*) dan pengguna (*guest*, *admin*, *top manager* dan sebagainya), *access control* seringkali dilakukan dengan menggunakan kombinasi *user*ID/*password* atau dengan menggunakan mekanisme lain (kartu, biometrik).
6. *Non-repudiation*
   Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan transaksi, sebagai contoh seseorang yang mengirimkan e-mail untuk memesan barang tidak dapat menyangkal bahwa dirinya telah mengirimkan e-mail tersebut.

3. *E-mail Security*

E-mail mungkin merupakan sistem yang paling populer digunakan untuk pertukaran informasi bisnis melalui internet atau jaringan komputer lainnya. Pada tingkat paling dasar, proses e-mail dapat dibagi menjadi dua komponen utama: (1) *mail server*, dimana *host* yang menyampaikan, memforward dan menyimpan e-mail; dan (2) *mail client*, yang merupakan *interface* untuk

pengguna dan memungkinkan pengguna untuk membaca, menulis, mengirim dan menyimpan e-mail.

4. Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ([SCH 1996], 1). Pengertian yang lain yaitu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, keutuhan data, otentikasi entitas dan otentitikasi sumber data ([MENZ 1997], 4). Dalam kriptografi terdapat dua konsep utama yakni enkripsi/deskripsi dan tanda tangan digital..

C. METODOLOGI PENELITIAN

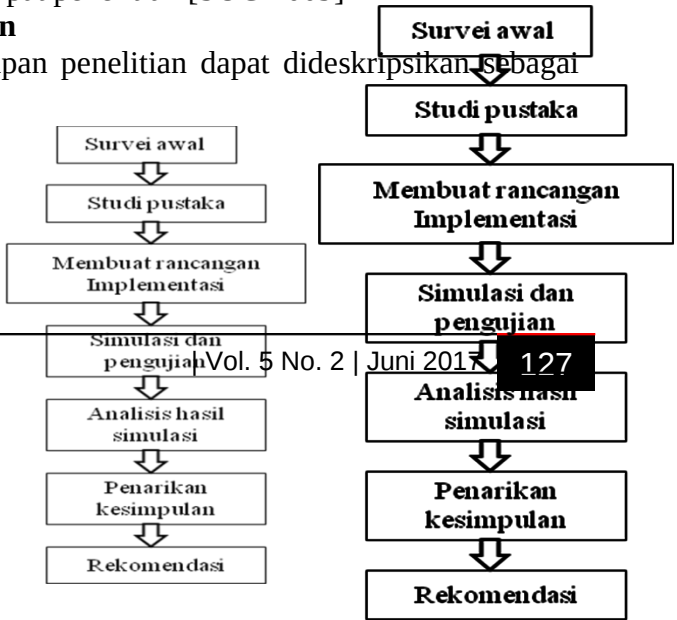
1. Metode Analisa Data

Dalam penelitian ini penulis memilih metode penelitian deskriptif kualitatif. Selain menggunakan metode deskriptif kualitatif, penelitian ini juga menggunakan metode simulasi untuk membuktikan efektivitas dari hasil rancangan implementasi yang dibuat.

Metode penelitian kualitatif digunakan digunakan untuk meneliti pada tempat yang alamiah, dan penelitian tidak membuat perlakuan, karena peneliti dalam mengumpulkan data bersifat *emic*, yaitu berdasarkan pandangan dari sumber data, bukan pandangan peneliti. Dalam penelitian kualitatif peneliti sebagai *human instrument* dan dengan teknik pengumpulan data *participant observation* (observasi berperan serta) dan *in depth overview* (wawancara mendalam), maka peneliti harus berinteraksi dengan sumber data. Walaupun penelitian kualitatif tidak membuat generalisasi, bukan berarti hasil penelitian kualitatif tidak dapat diterapkan di tempat lain. Generalisasi dalam penelitian kualitatif disebut *transferability* dalam bahasa Indonesia dinamakan keteralihan. Maksudnya adalah bahwa hasil penelitian kualitatif dapat ditransferkan atau diterapkan di tempat lain, manakala kondisi tempat lain tersebut tidak jauh berbeda dengan tempat penelitian [SUG 2009]

2. Langkah Penelitian

Tahapan-tahapan penelitian dapat dideskripsikan sebagai berikut:



Gambar 2. Alur Langkah Penelitian

Penjelasan dari deskripsi langkah penelitian tersebut adalah:

1. Melakukan survey awal
   Langkah ini bertujuan untuk mengetahui kondisi pelaksanaan transaksi informasi melalui layanan e-mail *online* yang dilakukan PT. Buana Jaya saat ini. Survei awal ini merupakan salah satu metode pengumpulan data. Survei awal dalam penelitian ini dilakukan dengan teknik wawancara dan observasi.
2. Melakukan Studi Pustaka
   Penelitian ini dimulai dengan melakukan studi pustaka yang berkaitan dengan pemanfaatan protokol S/MIME pada layanan e-mail. Studi pustaka dilakukan dengan mempelajari konsep dasar e-mail, *e-mail security*, aspek keamanan jaringan komputer, kriptografi, enkripsi/deskripsi, tanda tangan digital, *Public Key Infrastructure* (PKI), sertifikat digital, MIME dan S/MIME.
3. Membuat Rancangan Implementasi
   Setelah menegtahui kondisi di lapangan, langkah selanjutnya adalah membuat rancangan pemanfaatan protokol S/MIME pada layanan e-mail bagi PT. Buana Jaya.
4. Simulasi dan Pengujian
   Pada tahap ini peneliti berfokus pada kegiatan simulasi dan pengujian keamanan e-mail dalam beberapa kondisi. Simulasi dilakukan dengan cara mentransaksikan (kirim/terima) pesan e-mail antar pengguna layanan , sedangkan pengujian keamanan dilakukan dengan cara melakukan penyadapan terhadap isi e-mail (*body* dan *attachment*) yang ditransaksikan selama simulasi. Alat bantu yang digunakan untuk pengujian keamanan e-mail adalah aplikasi LAN *Detective Professional* dan *Wireshark.*

Berikut adalah kondisi yang akan disimulasikan dan diuji keamanannya oleh peneliti:

a. Sebelum menggunakan S/MIME

Peneliti melakukan simulasi transaksi (kirim/terima) e-mail yang belum menerapkan S/MIME. Kemudian peneliti menyadap *body* dan *attachment* e-mail yang ditransaksikan untuk membuktikan bahwa e-mail yang belum menggunakan S/MIME adalah tidak aman, dengan kata lain isi pesan dapat dibaca dan dipahami.

b. Setelah menggunakan S/MIME

1. Dengan mengaktifkan fitur *digital signature*
   Peneliti melakukan simulasi transaksi (kirim/terima) e-mail yang menerapkan S/MIME dengan mengaktifkan fitur *digital signature* namun tanpa mengaktifkan fitur enkripsi. Kemudian peneliti menyadap *body* dan *attachment* e-mail yang ditransaksikan untuk membuktikan aspek keamanan e-mail yang dapat terpenuhi.
2. Dengan mengaktifkan fitur enkripsi
   Peneliti melakukan simulasi transaksi (kirim/terima) e-mail yang telah menerapkan S/MIME dengan mengaktifkan fitur enkripsi namun tanpa mengaktifkan fitur *digital signature*. Kemudian peneliti menyadap *body* dan *attachment* e-mail yang ditransaksikan untuk membuktikan aspek keamanan e-mail yang dapat terpenuhi.
3. Dengan mengaktifkan fitur *digital signature* dan enkripsi
   Peneliti melakukan simulasi transaksi (kirim/terima) e-mail yang belum menerapkan S/MIME dengan mengaktifkan fitur *digital signature* dan enkripsi. Kemudian peneliti menyadap *body* dan *attachment* e-mail yang ditransaksikan untuk membuktikan aspek keamanan e-mail yang dapat terpenuhi.
5. Analisis Hasil Simulasi
   Melakukan perbandingan keamanan pada layanan e-mail setelah melakukan simulasi sebelum dan sesudah menggunakan S/MIME.
6. Penarikan Kesimpulan
   Penarikan kesimpulan ini bertujuan untuk menjelaskan kesesuaian hasil rancangan untuk diterapkan pada aplikasi e-mail PT. Buana Jaya, jalan atau tidaknya protokol S/MIME jika diterapkan, beserta pemenuhan, terhadap aspek keamanan dalam rancangan implementasi S/MIME.

7. Rekomendasi
   Tahapan ini bertujuan untuk mengusulkan rancangan implementasi S/MIME untuk diterapkan pada sistem e-mail PT. Buana Jaya.

D PEMBAHASAN

1. Simulasi dan Pengujian Keamanan Transaksi E-mail Non Protokol S/MIME

Pada bagian ini peneliti berfokus kepada simulasi transaksi e-mail antar *account* e-mail milik entitas/*user* tanpa menggunakan protokol S/MIME, dimana e-mail tersebut dilengkapi dengan *attachment* file yang berformat dokumen (*.doc), gambar (*.jpg). Di saat yang bersamaan peneliti menguji keamanan terhadap simulasi transaksi e-mail yang sedang dilakukan dengan cara menyadap *traffic* data selama transaksi berlangsung dengan tujuan membuktikan aman atau tidaknya transaksi e-mail tanpa menggunakan protokol S/MIME. Alat bantu yang peneliti gunakan untuk pengujian keamanan adalah aplikasi "LAN *Detective Professional*".

Tabel 1. Hasil Simulasi Transaksi E-mail Non S/MIME

***Account* E-mail Pengirim**	***Account* E-mail Penerima**	**Proses Transaksi E-mail non S/MIME**
direktur.ti@sim.ictlab.org	kadep.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Sukses Sukses Sukses Sukses Sukses Sukses
kadep.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Sukses Sukses Sukses Sukses Sukses Sukses
senman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org kadep.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Sukses Sukses Sukses Sukses Sukses Sukses

	asman.ti@sim.ictlab.org	
	asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	
kadep.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca
senman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org kadep.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca
man.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org kadep.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca
asman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca

man.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org kadep.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca
asman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca
	kadep.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	
senstaff.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org kadep.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca
junstaff.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org kadep.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Dapat Dibaca

2. Simulasi dan Pengujian Transaksi E-mail Menggunakan Protokol S/MIME

Pada bagian ini peneliti berfokus kepada simulasi transaksi e-mail antar *account* e-mail milik entitas/*user* menggunakan protokol S/MIME, dimana e-mail tersebut dilengkapi dengan *attachment* file yang berformat dokumen (*.doc), gambar (*.jpg) dan video (*.3gp). Di saat yang bersamaan peneliti menguji keamanan terhadap simulasi transaksi e-mail yang sedang dilakukan dengan cara menyadap *traffic* data selama transaksi berlangsung dengan tujuan membuktikan aman atau tidaknya transaksi e-mail menggunakan protokol S/MIME. Alat bantu yang peneliti

gunakan untuk pengujian keamanan adalah "LAN *Detective Professional*".

Tabel 3. Hasil Simulasi Transaksi E-mail Menggunakan S/MIME antar *account* e-mail

***Account* E-mail Pengirim**	***Account* E-mail Penerima**	**Proses Transaksi E-mail dengan S/MIME**
direktur.ti@sim.ictlab.org	kadep.ti@sim.ictlab.org	Sukses
	senman.ti@sim.ictlab.org	Sukses
	man.ti@sim.ictlab.org	Sukses
	asman.ti@sim.ictlab.org	Sukses
	senstaff.ti@sim.ictlab.org	Sukses
	junstaff.ti@sim.ictlab.org	Sukses
kadep.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org	Sukses
	senman.ti@sim.ictlab.org	Sukses
	man.ti@sim.ictlab.org	Sukses
	asman.ti@sim.ictlab.org	Sukses
	senstaff.ti@sim.ictlab.org	Sukses
	junstaff.ti@sim.ictlab.org	Sukses
senman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org	Sukses
	kadep.ti@sim.ictlab.org	Sukses
	man.ti@sim.ictlab.org	Sukses
	asman.ti@sim.ictlab.org	Sukses
	senstaff.ti@sim.ictlab.org	Sukses
	junstaff.ti@sim.ictlab.org	Sukses
man.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org	Sukses
	senman.ti@sim.ictlab.org	Sukses
	kadep.ti@sim.ictlab.org	Sukses
	asman.ti@sim.ictlab.org	Sukses
	senstaff.ti@sim.ictlab.org	Sukses
	junstaff.ti@sim.ictlab.org	Sukses
asman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org	Sukses
	senman.ti@sim.ictlab.org	Sukses
	man.ti@sim.ictlab.org	Sukses
	kadep.ti@sim.ictlab.org	Sukses
	senstaff.ti@sim.ictlab.org	Sukses
	junstaff.ti@sim.ictlab.org	Sukses

senstaff.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org kadep.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Sukses Sukses Sukses Sukses Sukses Sukses
junstaff.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org kadep.ti@sim.ictlab.org	Sukses Sukses Sukses Sukses Sukses Sukses

Berikut adalah hasil dari pengujian keamanan transaksi e-mail antar *account* e-mail milik entitas/*user* PT. Buana Jaya dengan menggunakan protokol S/MIME:

Tabel 4. Hasil Pengujian Keamanan Transaksi E-mail Menggunakan S/MIME antar *account* e-mail

***Account* E-mail Pengirim**	***Account* E-mail Penerima**	**Hasil Pengujian Keamanan (Penyadapan)**
direktur.ti@sim.ictlab.org	kadep.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Tidak Dapat Dibaca
kadep.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Tidak Dapat Dibaca
senman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org kadep.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Tidak Dapat Dibaca

man.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org kadep.ti@sim.ictlab.org asman.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Tidak Dapat Dibaca
asman.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org kadep.ti@sim.ictlab.org senstaff.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Tidak Dapat Dibaca
senstaff.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org kadep.ti@sim.ictlab.org junstaff.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Tidak Dapat Dibaca
junstaff.ti@sim.ictlab.org	direktur.ti@sim.ictlab.org senman.ti@sim.ictlab.org man.ti@sim.ictlab.org asman.ti@sim.ictlab.org	Semua Konten E-mail dan *Attachment* File Tidak Dapat

3. Hasil Perbandingan Pengujian Keamanan Transaksi E-mail

Berdasarkan hasil pengujian keamanan terhadap simulasi transaksi e-mail yang sebelumnya telah dilakukan oleh peneliti, dimana jika dibandingkan hasil pengujian keamanan tersebut maka sangat jelas terlihat bahwa transaksi e-mail yang mengimplementasikan protokol S/MIME keamanannya akan lebih terjamin. Hal ini terjadi karena selama berlangsungnya proses transaksi e-mail seluruh konten e-mail beserta *attachment* file akan dienkripsi dan ditandatangani oleh sertifikat digital, sehingga seorang *attacker* yang melakukan kegiatan penyadapan hanya akan mendapatkan rangkaian karakter acak yang tidak dapat dimengerti atau dipahami maknanya.

4. Implikasi Penelitian

Berdasarkan pada penelitian yang telah dilaksanakan, maka beberapa implikasi yang akan terjadi apabila rancangan implementasi S/MIME pada layanan e-mail ini diterapkan pada PT. Buana Jaya meliputi aspek sistem, manajerial dan penelitian lanjutan.

E. KESIMPULAN DAN SARAN

Kesimpulan

Dari uraian yang telah dipaparkan pada bab-bab sebelumnya, maka dapat diambil kesimpulan sebagai berikut:

1. Teknologi protokol S/MIME merupakan solusi alternative yang sesuai bagi PT. Buana Jaya untuk mengamankan layanan e-mail dalam mentransaksikan data/informasi antar entitas/*user*, namun sampai dengan saat ini PT. Buana Jaya belum memiliki rancangan implementasi protokol S/MIME yang nantinya dapat dilaksanakan.
2. Peneliti melakukan perancangan implementasi protokol S/MIME yang sesuai dengan kebutuhan PT. Buana Jaya meliputi topologi infrastruktur e-mail yang menerapkan protokol S/MIME serta tahapan perencanaan implementasi dari rancangan tersebut. Dalam rancangan implementasi protokol S/MIME pada layanan e-mail yang peneliti usulkan, telah ditentukan bahwa rancangan tersebut tidak akan mengubah konfigurasi *mail server* yang saat ini sedang berjalan. Selain itu, teknologi protokol S/MIME yang diterapkan juga bersifat *open source* dan *multiplatform* OS. Saat ini PT. Buana Jaya telah memiliki infrastruktur e-mail mandiri yang nantinya dapat mengimplementasikan teknologi pengamanan e-mail menggunakan protokol S/MIME.

3. Dari hasil simulasi yang dilakukan oleh peneliti, didapatkan bahwa transaksi e-mail yang menerapkan protokol S/MIME dapat sukses dilakukan. Hal ini terlihat dari berhasilnya kegiatan kirim dan terima data/informasi via e-mail dengan mengaktifkan fitur enkripsi dan tanda tangan digital. Aspek-aspek keamanan informasi yang meliputi *confidentiality, integrity, authentication* dan *non-repudiation* dapat terpenuhi oleh teknologi protokol S/MIME. Sedangkan dari hasil perbandingan pengujian keamanan, didapatkan bahwa keamanan transaksi e-mail yang menggunakan protokol S/MIME keamanannya lebih terjamin.

Saran

Berdasarkan pada penelitian yang telah dilakukan, maka beberapa hal yang disarankan adalah sebagai berikut:

1. Ketika rancangan implementasi protokol S/MIME ini akan direalisasikan, maka perlu adanya kebijakan dari pimpinan PT. Buana Jaya yang menjelaskan kualifikasi SDM sebagai

administrator CA yang diijinkan untuk melakukan manajemen protokol S/MIME.

2. Selain membutuhkan kebijakan kualifikasi SDM, ketika rancangan implementasi protokol S/MIME ini akan direalisasikan maka hal lain yang diperlukan adalah adanya kebijakan dari pimpinan yang mengharuskan setiap entitas/*user* yang terlibat dalam transaksi data/informasi menggunakan S/MIME untuk merahasiakan data/informasi yang ditransaksikan. Hal ini bertujuan agar tidak terjadinya kebocoran yang disebabkan oleh kelalaian entitas/*user*.
3. Perlu dilakukan penelitian lebih lanjut dari segi efisiensi dan efektivitas pada rancangan implementasi protokol S/MIME yang dibuat oleh peneliti.

DAFTAR PUSTAKA

[ADAMS 2000] C. Adams, and S. Lloyd, *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*, Indianapolis: Macmillan Technical Publishing, 2000.

[BANDAY 2011] Banday, M. Tariq, *International Journal of Distributed and Parallel Systems* (IJDPS): *Effectiveness and Limitations of E-mail Security Protocols*, 2011.

[DEPDAG 2001] Departemen Perindustrian dan Perdagangan, Naskah Akademik Rancangan Undang-Undang tentang Tanda Tangan Elektronik dan Transaksi Elektronik, Jakarta: Dirjen Perdagangan Dalam Negeri, 2001.

[GILL 2011] Gill, Sunny, etc., *International Journal of Computer Trends and Technology: E-mail Security Protocol*, 2011.

[HAS 2011] Hasad, Andi, Peningkatan Layanan Keamanan S/MIME, Bogor: Institut Pertanian Bogor, 2011.

[MOR 2007] C. Moris and S. Smith, *Towards Usefully Secure E-mail*, New York: IEEE *Technology and Society Magazine*, pp. 25-34., 2007.

[MUNIR 2006] Munir, Rinaldi, Pengantar Kriptografi, Bandung: Penerbit Informatika, 2006.

[NOV 2009] Novasandro, Ridzky, dkk. 2008. *Prinsip Kerja Protokol-*

Protokol Electronic Mail. http://te.ugm.ac.id/. 23 Mei 2012.

[QOYY 2008] Qoyyim, Ibnul, Implementasi Algoritma Kunci Publik Kriptografi Kurva Eliptik pada Aplikasi Email Mozila Thuderbird, 2008.

[SCH 1996] Schneier, Bruce, *Applied Cryptography*, U.S America: John Wiley & Sons, inc, 1996.

[SET 2010] Setyorini, Fitri, *E-mail Security* (Bahan Ajar), Institut Teknologi Sepuluh Nopember, 2010.

[SUG 2009] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif dan R&D, Jakarta: Alfabeta, 2009.

[SUM 2007] Sumarkidjo, dkk., Jelajah Kriptologi, Jakarta: Lembaga Sandi Negara RI, 2007.