p-ISSN: 2406-7768
e-ISSN: 2581-2181

Rancangan Implementasi Protokol S/Mime Pada Layanan E-mail Sebagai Upaya Peningkatan Jaminan Keamanan Dalam Transaksi Informasi Secara *Online* (Studi Kasus : PT. XYZ)

Reni Haerani[1], Zaenal Muttaqin[2]
[1]*Program Studi Manajemen Informatika Politeknik PGRI Banten*
Bussiness Square Blok C-16, Kedaleman, Cilegon Banten 42423
[1]Renihaerani27@yahoo.com

[2]*Jurusan Sistem Informasi Fakultas Teknologi Informasi Universitas Serang Raya*
Jln. Raya Cilegon Serang – Drangong Kota Serang
[2]d.zaey.vu@gmail.com

Abstrak - Perkembangan teknologi informasi memberikan dampak dalam segala aspek kehidupan manusia, yaitu cara berkomunikasi manusia yang awalnya bersifat konvensional menjadi digital. E-mail merupakan layanan yang disediakan sistem teknologi informasi sebagai sarana untuk bertransaksi informasi di dunia digital. Berkomunikasi menggunakan e-mail memiliki banyak kelebihan namun di sisi lain rentan terhadap kegiatan digital attacker, seperti penyadapan. Security adalah kunci untuk pengamanan informasi yang dibawa oleh *e-mail.* PT. XYZ merupakan organisasi yang bergerak di bidang bisnis yang menangani infrastruktur TI di kalangan instansi pemerintah maupun swasta, yang mana kesehariannya informasi rahasia ditransaksikan menggunakan *e-mail online*. S/MIME merupakan salah satu alternatif pengamanan yang dapat diimplementasikan pada e-mail. Hasil akhir dari penelitan ini berupa rancangan implementasi protokol S/MIME pada layanan e-mail bagi PT. XYZ yang menerapkan teknik kriptografi berupa tanda tangan digital dan/atau enkripsi yang terbukti dapat memenuhi aspek keamanan informasi. Dengan mengimplementasikan S/MIME, aspek information security seperti *confidentiality, integrity, authentication* dan *non-repudiation* yang diharapkan oleh PT. XYZ dapat terpenuhi.

***Kata Kunci**: e-mail, digital attacker, security, S/MIME, information security*

I. PENDAHULUAN

Perkembangan komunikasi digital semakin pesat setelah munculnya internet. Internet memberikan banyak layanan yang memungkinkan manusia saling bertukar informasi tanpa mengenal jarak dan waktu.

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. Meskipun menjadi sarana transaksi informasi yang handal dan banyak digunakan, mekanisme pengiriman e-mail umumnya dilakukan melalui internet yang merupakan jalur publik sehingga memungkinkan terjadinya serangan oleh *digital attacker* seperti penyadapan dan modifikasi informasi. Proses transaksi informasi melalui e-mail pada dasarnya menggunakan protokol *plaintext*, sehingga jika terjadi penyadapan akan menyebabkan kebocoran informasi, dengan kata lain mengancam kerahasiaan informasi dari e-mail tersebut.

Selain terkendala pada aspek kerahasiaan informasi, penerima e-mail tidak dapat memastikan keaslian sumber pesan, untuk mengetahui bahwa e-mail tersebut memang

p-ISSN: 2406-7768
e-ISSN: 2581-2181

berasal dari orang yang diajak berkomunikasi. Karena e-mail tidak memiliki layanan untuk memverifikasi pengirim e-mail, maka pengirim pada suatu waktu dapat menyangkal bahwa dirinya tidak pernah mengirim e-mail tersebut. Kedua kendala tersebut dapat diatasi dengan teknik kriptografi berbasis sertifikat digital kunci publik (*public key*) atau yang dikenal sebagai protokol

S/MIME karena terdapat dua proses yang dilakukan yaitu proses enkripsi sebagai solusi dari ancaman kerahasiaan informasi dan proses *digital signature* sebagai solusi untuk melakukan verifikasi terhadap pengirim e-mail.

Prinsip kerja S/MIME adalah mengirimkan informasi yang ditandatangani menggunakan *private key* pengirim dan kemudian mengenkripsinya menggunakan *public key* penerima, selanjutnya informasi tersebut dikirim ke penerima secara *point to point* melalui *mail server*, setelahnya pihak penerima akan mendekripsinya menggunakan *private key* penerima dan diotentikasi keaslian pengirimnya dengan *public key* pengirim. Proses *digital signature* dan enkripsi hanya terjadi antar user yang menggunakan e-mail S/MIME, tidak terjadi pada mail server.

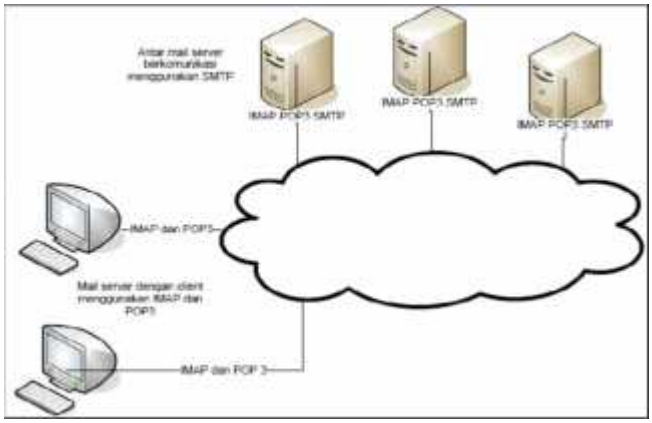
PT. XYZ merupakan organisasi bisnis yang menangani infrastruktur TI di kalangan instansi pemerintah dan swasta. Dalam melakukan proses komunikasi dan koordinasi, pimpinan dan karyawan PT. XYZ menggunakan layanan e-mail untuk saling bertransaksi informasi. Data atau informasi yang biasanya dikomunikasikan bersifat terbatas dan rahasia seperti proyek perusahaan, nama pelanggan, jenis proyek, nama proyek, dana proyek, pihak yang terlibat dalam proyek, dan lain-lain. Informasi yang demikian tentunya akan berdampak buruk apabila jatuh ke tangan pihak yang tidak berhak, contohnya pihak pesaing bisnis.

E-mail

Electronic 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.

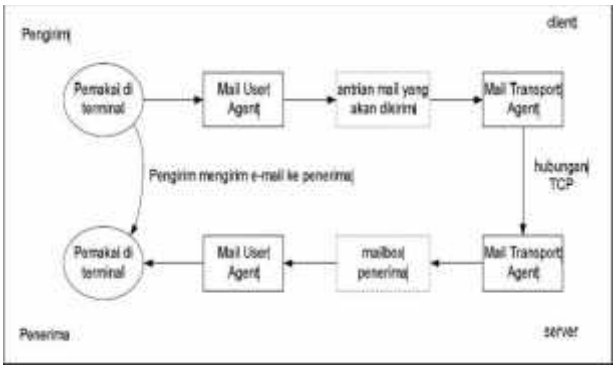
Pengiriman e-mail tidak menggunakan kertas melainkan menggunakan suatu aplikasi berbentuk program komputer, dengan media komunikasi jaringan. E-mail memungkinkan seseorang menuliskan beberapa teks, mengidentifikasi pihak yang ingin dikirimi pesan dengan menuliskan alamat e-mail seseorang di bagian atas dan dikirimkan ke alamat tersebut.

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 protokol pada e-mail

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*) dan pembacaannya menggunakan protokol POP (*Post Office 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.



p-ISSN: 2406-7768
e-ISSN: 2581-2181

Gambar .2. Komponen konseptual sistem e-mail

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.

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.

3. *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*) di mana server biasanya dengan mengirim *request* yang berkelanjutan atau permintaan di luar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan 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.

*6. Non-repudiatio*n

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan transaksi, Penggunaan tanda tangan digital, sertifikat, dan teknologi kriptografi secara umum dapat menjaga aspek ini dan tentu saja harus didukung dengan aspek hukum sehingga status dari tanda tangan itu jelas dan legal.

E-mail Security

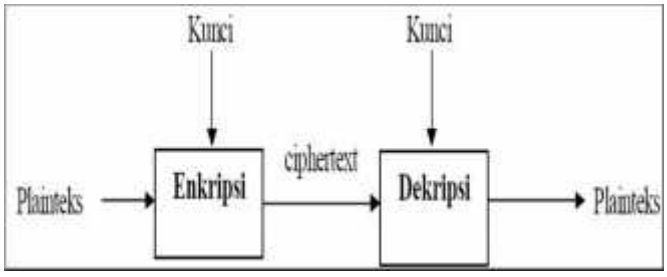
E-mail mungkin merupakan sistem yang paling populer digunakan untuk pertukaran informasi bisnis melalui internet (atau jaringan komputer lainnya). Pada tingkat paling dasar, proses e-mail dapat dibagi menjadi dua komponen utama: (1) *mail server*, di mana *host* yang menyampaikan, mem-*forward* dan menyimpan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

Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan [3]. Pengertian yang lain yaitu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, keutuhan data, otentikasi entitas dan otentikasi sumber data ([MENZ 1998], 4). Dalam kriptografi terdapat dua konsep utama yakni enkripsi/dekripsi dan tanda tangan digital.

Enkripsi/Dekripsi

Enkripsi adalah proses mengolah informasi/data (*plaintext*) menjadi bentuk yang hampir tidak dikenali (*ciphertext*) dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali *ciphertext* menjadi *plaintext*.



Gambar 3. Diagram proses enkripsi dan dekripsi

p-ISSN: 2406-7768
e-ISSN: 2581-2181

Menurut taksonominya, pada dasarnya kriptografi terbagi dalam 3 (tiga) kategori yaitu *unkeyed primitives*, *symmetric key primitives* dan *asymmetric key primitives* [5].

Tanda Tangan Digital

Tanda tangan digital (*digital signature*) adalah bentuk tiruan tanda tangan konvensional ke dalam bentuk digital. Namun bukan file hasil dari scan tanda tangan kertas. Bentuk tanda tangan digital adalah berupa byte-byte yang jika diperiksa bisa digunakan untuk memeriksa apakah suatu dokumen digital, termasuk e-mail, benar berasal dari orang tertentu atau tidak. Dengan tanda tangan digital maka dapat di ketahui integritas dari suatu file.

MIME

MIME (*Multipurpose Internet Mail Extension*) adalah standar format e-mail, yang merupakan perluasan untuk kerangka RFC 5321 yang dimaksudkan untuk mengatasi beberapa masalah dan keterbatasan penggunaan SMTP atau protokol transfer mail lain dan RFC 5322 untuk mail elektronik.

S/MIME

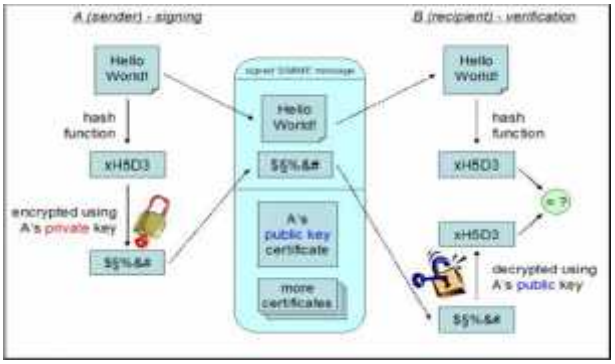
S/MIME (*Secure/Multipurpose Internet Mail Extension*) adalah peningkatan keamanan standar format e-mail internet MIME, yang didasarkan pada teknologi dari keamanan data RSA. S/MIME didefinisikan dalam sejumlah dokumen, yang paling penting adalah RFC 3369, 3370, 3850 dan 3851.

Tabel 1. Tipe Konten S/MIME

Tipe	Subtipe	Parameter S/MIME	Deskripsi
Multipart	Signed		Pesan ditandatangani dalam dua bagian : pesan dan tanda tangan.
Application	pkcs7-mime	signedData	Menandatangani entitas S/MIME
	pkcs7-mime	envelopeData	Mengenkripsi entitas S/MIME
	pkcs7-mime	Degenerate signedData	Entitas hanya berisi sertifikat kunci publik
	pkcs7-mime	compressedData	Mengkompres entitas S/MIME
	pkcs7-signature	signedData	Tipe konten dari sub bagian tanda tangan pada pesan multipart/signed.

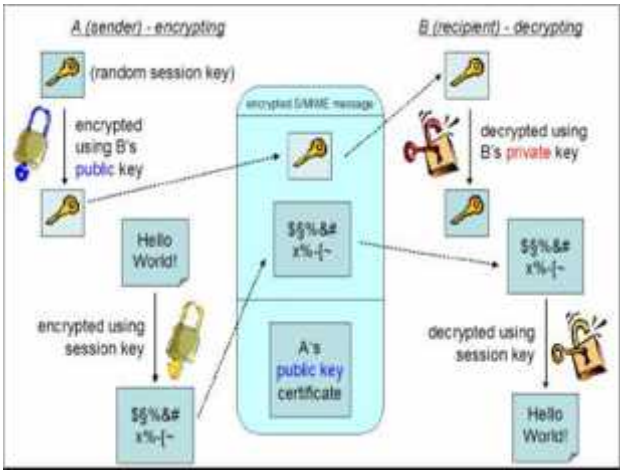
S/MIME melindungi entitas MIME dengan tanda tangan, enkripsi, atau keduanya. Entitas MIME merupakan pesan keseluruhan (kecuali untuk *header* RFC 5322), jika tipe konten MIME *multipart*, maka entitas MIME terdiri dari satu atau lebih dari subbagian pesan entitas MIME yang disusun menurut aturan normal untuk pesan MIME. Pesan yang dikirimkan pada S/MIME akan mengalami proses penandatanganan dan enkripsi sebagai satu kesatuan proses tak terpisahkan, kemudian setelah sampai ke penerima dilakukan proses verifikasi tanda tangan digital dan dekripsi pesan untuk kemudian pesan akan dapat dibaca oleh penerima.

a. Proses penandatanganan dan verifikasi pesan



Gambar 4. Proses penandatanganan pesan S/MIME

b. Proses enkripsi dan dekripsi pesan



Gambar 5. Proses enkripsi/dekripsi pesan S/MIME

Penandatanganan dan enkripsi pesan sebagai satu kesatuan proses, sehingga pesan S/MIME yang dikirimkan dari

p-ISSN: 2406-7768
e-ISSN: 2581-2181

pengirim ke penerima adalah berupa pesan terenkripsi dan pesan yang tertandatangani secara digital.

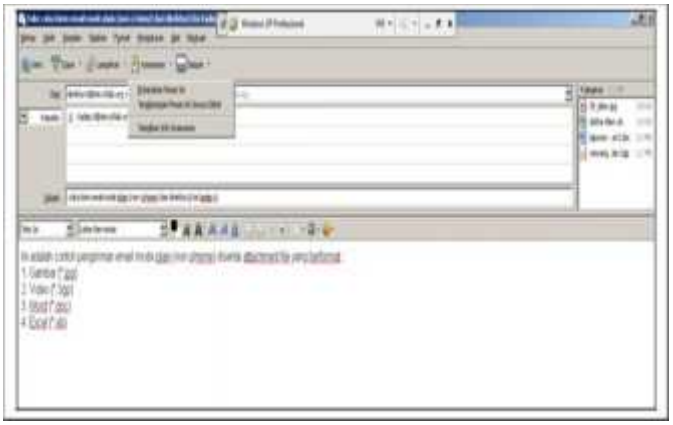
II. METODOLOGI PENELITIAN

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.

III. HASIL DAN PEMBAHASAN

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

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) dan video (*.3gp). 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*".



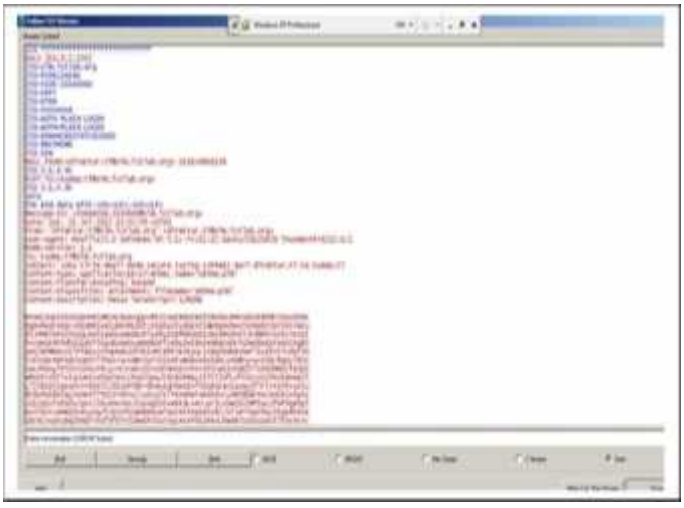
Gambar 6. Menonaktifkan protokol S/MIME sebelum transaksi e-mail

Gambar 7. Penyadapan transaksi e-mail

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

Simulasi transaksi e-mail antar *account* e-mail milik entitas/*user* menggunakan protokol S/MIME, dimana e-mail tersebut tersebut dilengkapi dengan *attachment* file yang berformat dokumen (*.doc), gambar (*.jpg) dan video (*.3gp). 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*".

Gambar 8. Sukses transaksi e-mail



Gambar 9. Bentuk konten e-mail menggunakan protokol S/MIME

p-ISSN: 2406-7768
e-ISSN: 2581-2181

Hasil Perbandingan Pengujian Keamanan Transaksi E-mail

Berdasarkan hasil pengujian keamanan terhadap simulasi transaksi e-mail, 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.

Analisis Keterkaitan Aspek-Aspek Keamanan Informasi pada S/MIME

Setelah simulasi dilakukan, maka dapat terlihat bagaimana bentuk format dan karakter yang muncul apabila dilakukan penyadapan menggunakan LAN *Detective Professional* dan membacanya menggunakan Wireshark. Berikut adalah
salah satu format pesan yang didapatkan dari hasil simulasi penyadapan:

```
From - Sat Jul 21 13:33:13 2012
X-Account-Key: account1
X-UIDL: 267.Hmm,5Z6o55VGh4wuIXj,yubOQl0=
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: direktur.ti@sim.ictlab.org
Received: from sim.ictlab.org (LHLO sim.ictlab.org) (192.168.10.15)
by sim.ictlab.org with LMTP; Sat, 21 Jul 2012 13:23:24 +0000 (UTC)
Received: from localhost (localhost [127.0.0.1])
        by sim.ictlab.org (Postfix) with ESMTP id 6C98F112546
        for <kadep.ti@sim.ictlab.org>; Sat, 21 Jul 2012 13:23:24 +0000 (UTC)
X-Virus-Scanned: amavisd-new at sim.ictlab.org
X-Spam-Flag: NO
X-Spam-Score: 1.343
X-Spam-Level: *
X-Spam-Status: No, score=1.343 tagged_above=-10 required=6.6

    tests=[ALL_TRUSTED=-1, BAYES_50=0.8, DATE_IN_PAST_06_12=1.543]
    autolearn=no


Received: from sim.ictlab.org ([127.0.0.1])
        by localhost (sim.ictlab.org [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id xq-k-mAxceh4 for <kadep.ti@sim.ictlab.org>; Sat, 21
        Jul 2012 13:23:23 +0000 (UTC)
Received: from [10.0.2.156] (unknown [192.168.10.20])
        by sim.ictlab.org (Postfix) with ESMTP id CE61411253C
        for <kadep.ti@sim.ictlab.org>; Sat, 21 Jul 2012 13:23:13 +0000 (UTC)
Message-ID: 500A4D1B.3030906@sim.ictlab.org
Date: Sat, 21 Jul 2012 13:32:59 +0700
From:"direktur.ti@sim.ictlab.org" direktur.ti@sim.ictlab.org
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:12.0) Gecko/20120428 Thunderbird/12.0.1
MIME-Version: 1.0
To: kadep.ti@sim.ictlab.org
Subject: coba kirim email mode secure (using s/mime) dari direktur.ti ke kadep.ti
Content-Type:application/pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: Pesan Terenkripsi S/MIME

MIAGCSqGSIb3DQEHA6CAMIACAQAxggV+MIICuwIBADCB
ojCBnDELMAkGA1UEBhMCSUQxDDA
KBgNVBAgTA0pLVDEUMBIGA1UEBxMLREtJIEpha2FydGEx
FzAVBgNVBAoTDnNpbS5pY3RsYWIub
3JnMRcwFQYDVQQLEw5zaW0uaWN0bGFiLm9yZzEPMA0GA
1UEAxMGdXNlckNBMSYwJAYJKoZIhv
```

Gambar 10. Format hasil penyadapan pesan S/MIME

Pesan pertama kali ditandatangani dan kemudian dienkripsi. Oleh karena itu, pesan terenkripsi dan tertandatangani terlihat persis seperti contoh pada Gambar 10, hanya penerima yang dapat mengetahui bahwa pesan tersebut telah ditandatangani secara digital. Karena terenkripsi, pesan tidak dapat dibaca oleh setiap orang yang tidak sah. Pesan teks terenkripsi (yang sebenarnya merupakan pesan yang ditandatangani terlebih dahulu dan kemudian dienkripsi) sebenarnya masih dapat diganti dengan pesan teks terenkripsi lainnya, namun tanda tangan digital (yang termasuk dalam bagian dari pesan terenkripsi yang isinya tidak dapat dimengerti oleh pengguna yang tidak sah) akan hilang selama proses tersebut.

IV. KESIMPULAN

1. Teknologi protokol S/MIME merupakan solusi alternatif yang sesuai bagi PT. XYZ untuk mengamankan layanan e-mail dalam mentransaksikan data/informasi antar entitas/*user*.
2. Melakukan perancangan implementasi protokol S/MIME yang sesuai dengan kebutuhan PT. XYZ,

p-ISSN: 2406-7768
e-ISSN: 2581-2181

meliputi topologi infrastruktur e-mail yang menerapkan protokol S/MIME serta tahapan perencanaan implementasi dari rancangan tersebut. Selain itu, teknologi protokol S/MIME yang diterapkan juga bersifat *open source* dan *multiplatform* OS.

3. Dari hasil simulasi yang dilakukan 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.

REFERENSI

[1] Novasandro, Ridzky, dkk. (2008). *Prinsip Kerja Protokol - Protokol Electronic Mail*. http://te.ugm.ac.id/. *23* Mei 2012.

[2] Cutra, Angga O., (2007). Aplikasi Pengamanan Pesan pada Mail *Client* dengan Menggunakan Algoritma CAST-128, Bandung: UNIKOM.

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

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

[5] Sumarkidjo, dkk.,(2007). Jelajah Kriptologi, Jakarta: Lembaga Sandi Negara RI.

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

[7] Moser, Heinrich, (2001). S/MIME, December 2001–January 2002.

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

[9] Forouzan, Behrouz A., (2008). *Cryptography and Network Security*, New York: Mc Graw Hill.

[10] Maryati, Kun, Sosilologi, (2005) Jakarta: ESIS.

[11] Menezes, Alfred J., Paul C. Van Oorschot, Scott A. Vanstone.,(1997). *Handbook of Applied Cryptography*, U.S America: CRC Press LLC.

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

[13] Qoyyim, Ibnul, (2008). Implementasi Algoritma Kunci Publik Kriptografi Kurva Eliptik pada Aplikasi Email Mozila Thunderbird.

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

[15] Stalling, William, (2005). *Cryptography and Network Security, Principles and Practices*, New York: Prentice Hall.

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

[17] Sumarkidjo, dkk.,(2007). Jelajah Kriptologi, Jakarta: Lembaga Sandi Negara RI.

[18] Burr, William, etc., (2006) NIST SP 800-63: *Electronic Authentication Guideline*, New York: NIST.