Jurnal String Vol. 2 No. 2 Desember 2017 **p-ISSN: 2527 - 9661**
e-ISSN: 2549 - 2837

IMPLEMENTASI PROTOKOL S/MIME PADA LAYANAN E-MAIL PENINGKATAN JAMINAN KEAMANAN SECARA *ONLINE PADA KANTOR PT. TAMMAR FRASTI*

Nahot Frastian[1]
Program Studi Informatika, Universitas Indraprasta PGRI[1]
nahotfrastian@gmail.com[1]

ABSTRAK

Implementasi teknologi sistem 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. TAMMAR FRASTI merupakan organisasi yang bergerak di bidang bisnis yang menangani infrastruktur Teknologi Informasi di kalangan perusahaan 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. TAMMAR FRASTI 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. TAMMAR FRASTI menjadi sukses.
Kata Kunci : Implementasi, *digital attacker* ,e- *security,* S/MIME mail, *information security.*

Abstract

Implementation of information system technology has been changing all aspects of human life, such as the human's way of communication that is initially conventional into digital way. E-mail is a service provided by information technology system as a means to exchange information digitally. Even though communicating using e-mail has many advantages, it is vulnerable to digital attackers, such as tapping. Security is the key to securing information contained in e-mail. PT. TAMMAR FRASTI is a business organization that deals with Information Technology infrastructure among private companies that exchange their daily confidential information using e-mail online. S/MIME is one of the alternative security that can be implemented in e-mail. The final result of this research is the design of S/MIME protocol implementation in e-mail service for PT. TAMMAR FRASTI applying cryptographic techniques in the form of digital signatures and / or encryption proven to meet the aspects of information security. By implementing S/MIME, information security aspects such as confidentiality, integrity, authentication and non-repudiation expected by PT. TAMMAR FRASTI may be successfully realized.
Keywords : *Implementation, digital attacker, e-security, S / MIME mail, information security.*

1. PENDAHULUAN

A. Latar Belakang

Perkembangan Teknologi Informasi 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 survei Internet World Stats pada internetworldstats.com mencapai 2.267.233.742 pengguna, dengan statistik tertinggi pengguna dari Asia mencapai 44,8% [1].

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 dari10 (91%) pengguna internet di Indonesia menggunakan e-mail *online* untuk kirim/terima (transaksi) informasi [2]. 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 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. Selain itu user yang tidak terdaftar sebagai grup terbatas tidak akan dapat melakukan komunikasi *secure* karena tidak memiliki sertifikat digital. PT. TAMMAR FRASTI merupakan organisasi bisnis yang menangani infrastruktur TI di kalangan instansi pemerintah dan swasta. Dalam melakukan proses komunikasi dan koordinasi, pimpinan dan karyawan PT. TAMMAR FRASTI 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.

Berangkat dari uraian di atas, peneliti menawarkan alternatif solusi berupa rancangan implementasi protokol S/MIME pada layanan e-mail untuk PT. TAMMAR FRASTI, yang mana bila rancangan tersebut diterapkan oleh PT. TAMMAR FRASTI maka peningkatan keamanan dalam bertransaksi informasi secara *online* akan terjamin.

B. Masalah Penelitian

Identifikasi Masalah

Berdasarkan latar belakang penelitian yang telah diuraikan, maka dapat di identifikasi permasalahan penelitian sebagai berikut:

1) PT. TAMMAR FRASTI melakukan transaksi informasi yang bersifat rahasia danterbatas menggunakan layanan e-mail *online* melalui jaringan publik (internet).

2) Internet rentan terhadap serangan penyadapan dan modifikasi pesan yang

dilakukan oleh *digital attacker*.
3) Dikarenakan PT. TAMMAR FRASTI mengirimkan e-mail melalui jaringan internet, maka rentan terhadap kebocoran informasi yang pada akhirnya dapat menimbulkan dampak buruk bagi perusahaan.
4) PT. TAMMAR FRASTI memerlukan alternatif solusi berupa rancangan pemanfaatan S/MIME yang dapat menjamin terpenuhinya aspek-aspek keamanan informasi khususnya e-mail yang meliputi *confidentiality, integrity, authentication* dan *non-repudiation*.

Batasan Masalah

Dengan adanya keterbatasan waktu dan sumber daya, maka penelitian Ini hanya membahas rancangan implementasi S/MIME pada layanan e-mail untuk PT. TAMMAR FRASTI, simulasi dan pengujian implementasi dari rancangan yang dibuat, serta perbandinganan keamanan dari hasil simulasi sebelum dan sesudah implementasi rancangan tersebut.

Rumusan Masalah

Dari identifikasi dan pembatasan masalah di atas, maka rumusan masalah penelitian ini dituangkan dalam bentuk pertanyaan penelitian sebagai berikut:
1) Solusi apakah yang dapat diterapkan untuk menjamin keamanan transaksi informasi berbasis layanan e-mail *online* bagi PT. TAMMAR FRASTI?
2) Bagaimanakah implementasi protokol S/MIME pada layanan e-mail bagi PT. TAMMAR FRASTI?
3) Bagaimanakah perbandingan keamanan dari hasil simulasi sebelum dan sesudah implementasi rancangan tersebut?

C. Tujuan dan Manfaat Penelitian

Penelitian ini bertujuan:
1) Mendeskripsikan rancangan implementasi S/MIME pada layanan e-mail *online* PT. TAMMAR FRASTI.
2) Membuktikan aspek keamanan yang dapat terpenuhi dalam transaksi informasi menggunakan e-mail yang menerapkan S/MIME.
3) Membandingkan keamanan transaksi informasi menggunakan e-mail *online* antara sebelum dan sesudah menerapkan S/MIME.

Manfaat dari penelitian adalah sebagai berikut:
1) Manfaat akademis Hasil dari penelitian diharapkan dapat mengembangkan pengetahuan,menambah wawasan kepustakaan pendidikan serta dapat menjadireferensi bagi penelitian selanjutnya.
2) Manfaat praktis Hasil dari penelitian diharapkan dapat menjadi bahan masukan bagi PT. TAMMAR FRASTI yang dapat diimplementasikan untuk meningkatkan keamanan komunikasi berbasis e-mail.

2. METODE 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. 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 [3].

Langkah Penelitian

Tahapan penelitian dapat di deskripsikan sebagai berikut:

1. Melakukan survei awal
   Langkah ini bertujuan untuk mengetahui kondisi pelaksanaan transaksi informasi melalui layanan e-mail*online* yang dilakukan PT. TAMMAR FRASTI 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 pemanfatan protokol S/MIME pada layanan e-mail. Studi pustaka dilakukandengan mempelajari konsep dasar e-mail, *e-mail security*, aspek keamanan jaringan komputer, kriptografi, enkripsi/dekripsi, tanda tangan digital, *Public Key Infrastructure* (PKI), sertifikat digital, MIME dan S/MIME.
3. Membuat rancangan implementasi
   Setelah mengetahui kondisi di lapangan, langkah selanjutnya adalah membuat rancangan pemanfaatan protokol S/MIME pada layanan e-mail bagi PT. TAMMAR FRASTI.

3. HASIL DAN PEMBAHASAN

Profil Perusahaan

PT. TAMMAR FRASTI merupakan organisasi yang bergerak di bidang teknologi informasi khususnya menangani infrastruktur jaringan di berbagai perusahaan swasta. PT. TAMMAR FRASTI dipimpin oleh seorang Direktur Utama. Dalam menjalankan proses bisnisnya, PT. TAMMAR FRASTI memiliki bagian yang khusus menangani *core business*-nya di bidang teknologi informasi, disebut Divisi IT. Dalam hal ini Divisi IT dipimpin oleh seorang Direktur IT. Berikut merupakan struktur organisasi pada lingkup Divisi IT.

Infrastruktur E-mail PT. TAMMAR FRASTI

Berdasarkan pengamatan peneliti, PT. TAMMAR FRASTI memiliki infrastruktur e-mail yang relatif memadai terlihat dari kelengkapan-kelengkapan jaringan yang digunakan, termasuk *bandwidth* internet yang dimiliki. Perangkat-perangkat jaringan yang dimiliki adalah *router, switch, firewall, access point* (AP), *mail gateway* dan *mail server*. Perangkat-perangkat tersebut digunakan oleh PT. TAMMAR FRASTI untuk koneksi internet dan diantaranya menjalankan layanan e-mail perusahaan.

Klasifikasi Data/Informasi PT. TAMMAR FRASTI

Dari diskusi yang dilakukan antara peneliti dengan Asisten Manajer TI, peneliti dapat mengklasifikasikan jenis data/informasi yang ditransaksikan melalui layanan e-mail. Klasifikasi dari jenis data/informasi yang ditransaksikan yaitu:

1. Data/informasi biasa

Adalah informasi yang bersifat umum dan semua pihak boleh mengetahui dan mempergunakannya.

2. Data/informasi rahasia

Adalah informasi yang bersifat terbatas dan tidak semua pihak berhak mengetahui dan mempergunakannya.

Data/informasi yang ditransaksikan memiliki format yang bermacam-macam jenisnya seperti teks (*word, excel, power point*, pdf, dll), gambar (.jpeg, .jpg, .png, bmp, .gif, dll), audio (.mp3, .wav, dll),

video (.3gp, .flv), dsb.

Proses Transaksi Data/Informasi

Proses transaksi (kirim/terima) data/informasi yang dilakukan oleh *user* PT. TAMMAR FRASTI adalah menggunakan layanan e-mail. *User* melakukan kirim/terima e-mail melalui aplikasi e-*mail client*, aplikasi tersebut yaitu *Mozilla Firefox*.

Mekanisme kirim/terima e-mail yang terjadi antar *user* PT. TAMMAR FRASTI adalah sebagai berikut:

Gambar 1. Tampilan *user interface* pada *Mozilla Firefox*

1.*User* pada sisi pengirim menjalankan aplikasi *Mozilla* dan mengklik fitur tulis pesan untuk mengirimkan e-mail.

2.Untuk mengirim e-mail, *user* memasukkan alamat tujuan/penerima dan subjek pesan, menulis teks pesan, serta melampirkan *attachment* file apabila dibutuhkan, kemudian mengirimkannya.

3. E-mail yang dikirimkan tersebut akan melalui *port* SMTP mail server PT.TAMMAR FRASTI, kemudian *mail server* akan memeriksa alamat tujuan/penerima, *mail server* juga akan menampung dan menyimpan data/informasi dari e-mail yang dikirimkan, selanjutnya *mail server* PT. TAMMAR FRASTI meneruskan e-mail yang dikirim ke POP3 tujuan/penerima. Alur diagram di bawah ini untuk memperjelas mekanisme kirim/terima e-mail antar *user* PT. TAMMAR FRASTI. Alur diagram di bawah ini untuk memperjelas mekanisme kirim/terima e-mail antar *user* PT. TAMMAR FRASTI: Gambar IV.3.

Alur diagram kirim/terima e-mail antar *user* PT. TAMMAR FRASTI Pengirim Jalankan Aplikasi Mozilla Thunderbird Klik Fitur Tulis Pesan Isi Alamat Tujuan/ Penerima, Subject, Teks Pesan, Lampirkan Attachment File (jika diperlukan) Kirim E-mail Mail Server SMTP Pengirim Mengecek Alamat Tujuan/Penerima Menampung & Menyimpan Data/ Informasi E-mail yang dikirimkan Meneruskan E-mail yang dikirimkan ke POP3 Penerima Penerima Jalankan Aplikasi Mozilla Thunderbird Notifikasi Inbox E-mail Membuka E-mail yang Masuk, Membaca pesan, Download Attachment (jika ada) Selesai .

Gambar 2. Tampilan *user interface* pada *Mozilla Firefox.*

Model Keamanan

Model keamanan yang telah dilakukan oleh PT. TAMMAR FRASTI untuk mengamankaninfrastruktur e-mail sampai dengan saat ini adalah dengan memasang *firewall*, *antivirus* dan *antispam* yang terintegrasi pada *mail server* TAMMAR FRASTI.

1. *Firewall*

Firewall digunakan untuk melindungi jaringan komputer yang ada di dalam PT. TAMMAR FRASTI. Hanya paket data yang di-*allow* yang boleh masuk/keluar jaringan.

PT. TAMMAR FRASTI, selain itu maka akan di-*block*.

PT. TAMMAR FRASTI berbasis

perangkat keras dan dipasang pada pintu gerbang (*gateway*) antara *router* dan LAN PT. TAMMAR FRASTI.

2. Antivirus
   Untuk melindungi infrastruktur e-mail terhadap serangan virus, trojan, *malware* maupun program jahat lainnya yang masuk ke dalam sistem e-mail maka digunakanlah antivirus yang telah terintegrasi di *mail server* PT.TAMMAR FRASTI.
3. Antispam
   Untuk melindungi *user* mendapatkan e-mail sampah maka digunakanlah anti spam yang terintegrasi di perangkat keras *mail server* PT.TAMMAR FRASTI.

Hambatan/Kendala yang Dihadapi

Hambatan/kendala yang dihadapi oleh PT. TAMMAR FRASTI dalam melakukan transaksi data/informasi melalui layanan e-mail yaitu belum adanya pengamanan dalam proses transaksi data/informasi antar *user*baik itu *user* yang berada di dalam maupun di luar kantor (*mobile network*) PT. TAMMAR FRASTI. Resikonya adalah data/informasi yang ditransaksikan dapat mudah disadap.

Pemilihan Protokol S/MIME

Seperti yang telah dijelaskan pada latar belakang masalah, protokol S/MIME merupakan salah satu solusi alternatif yang sesuai untuk diimplementasikan pada layanan e-mail bagi PT. TAMMAR FRASTI dengan alasan sebagai berikut:

1. PT. TAMMAR FRASTI telah memiliki infrastruktur jaringan internet.
2. Tidak diperlukan biaya tambahan untuk mengimplementasikan S/MIME karena aplikasi yang dibutuhkan bersifat *open source* dan *multiplatform* OS.
3. Investasi S/MIME lebih ringan daripada pengadaan jaringan pribadi (WAN) maupunVPN.

4. SIMPULAN

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

1. Penelitian Uraian simpulan teknologi protokol S/MIME merupakan solusi alternatif yang sesuai bagi PT. TAMMAR FRASTI untuk mengamankan layanan e-mail dalammentransaksikandata/informasi antar entitas/*user*, namun sampai dengan saat ini PT. TAMMAR FRASTI belum memiliki rancangan implementasi protokol S/MIME yang nantinya dapat dilaksanakan.
2. Peneliti melakukan perancangan implementasi protokol S/MIME yang sesuai dengan kebutuhan PT. TAMMAR FRASTI, meliputi topologi infrastruktur e-mail yang menerapkan protokol S/MIME serta tahapan implementasi dari rancangan tersebut. Dalam rancangan implementasi protokol S/MIME pada layanan e-mail yang peniliti 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. TAMMAR FRASTI telah memiliki infrastruktur e-mail mandiri yang nantinya dapat mengimplementasikan teknologi pengamanan e-mail menggunakan protokol S/MIME.
3. 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.

Saran

Penelitian yang telah dilakukan, maka beberapa hal yang disarankan adalah sebagai berikut:

1. Implementasi protokol S/MIME ini akan direalisasikan, maka perlu adanya kebijakan dari pimpinan PT. TAMMAR FRASTI yang menjelaskan kualifikasi SDM sebagai administrator CA yang diijinkan untuk melakukan manajemen protokol S/MIME.
2. 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 yangdisebabkan oleh kelalaian entitas/*user*.
3. Penelitian lebih lanjut dari segi efisiensi dan efektifitas pada rancangan implementasi protokol S/MIME yang dibuat oleh peneliti.

DAFTAR PUSTAKA

[1] Internet World Stats. 2011. *Internet Usage Statistics.* http://www.internetworldstats.com/stats.htm. 25 Mei 2012

[2] Ipsos. 2012. *Most Global Internet Users Turn to the Web for Emails (85%) and Social Networking Sites (62%).* http://www.ipsos-na.com/. 25 Mei 2012.

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

[4] C. Adams, S. Farrel, RFC 2510:*Internet X.509 Public Key Infrastructure Certificate Management Protocols,* California: IETF, 1999.

[5] C. Adams, and S. Lloyd, *Infrastructure: Concepts, Standards, and Deployment Considerations*, Indianapolis: Macmillan Technical Publishing, 2000.

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

[7] R. Barker, Elain, etc., NIST SP 800-21:*Guideline for Implementing Cryptography In the Federal Government*, New York: NIST,2005.

[8] Anonim.2008. *DRM Technologies-DRM (Part 2).* 2012.

[9] Chernick, C. Michael, NIST SP 800-49: Federal S/MIME V3*Client Profile*, New York: NIST, 2002.

[10] Cutra, Angga O., Aplikasi Pengamanan Pesan pada Mail dengan menggunakan Algoritma CAST-128, Bandung: UNIKOM,2007.

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

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

[13] S. Garfinkel. 2009. Signed, *Dealed and Delivered*, *CSO Online*.2012.

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

.