Perpustakaan Universitas Budi Luhur

RANCANGAN IMPLEMENTASI PROTOKOL S/MIME PADA LAYANAN E-MAIL SEBAGAI UPAYA PENINGKATAN JAMINAN KEAMANAN DALAM TRANSAKSI INFORMASI SECARA *ONLINE*: STUDI KASUS PT. XYZ

TESIS

Oleh :
Aeni Jamilia
1011600846

PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2012

Perpustakaan Universitas Budi Luhur

RANCANGAN IMPLEMENTASI PROTOKOL S/MIME PADA LAYANAN E-MAIL SEBAGAI UPAYA PENINGKATAN JAMINAN KEAMANAN DALAM TRANSAKSI INFORMASI SECARA *ONLINE*: STUDI KASUS PT. XYZ

TESIS

Diajukan untuk memenuhi salah satu persyaratan memperoleh gelar Magister Ilmu Komputer

Oleh:

Aeni Jamilia
1011600846

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2012

Perpustakaan Universitas Budi Luhur

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : AENI JAMILIA

NIM : 1011600846

Program Studi : MAGISTER ILMU KOMPUTER (MKOM)

Program : PASCASARJANA

menyatakan bahwa TESIS yang berjudul:

RANCANGAN IMPLEMENTASI PROTOKOL S/MIME PADA LAYANAN E-MAIL SEBAGAI UPAYA PENINGKATAN JAMINAN KEAMANAN DALAM TRANSAKSI INFORMASI SECARA ONLINE : STUDI KASUS PT. XYZ

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 3 SEPTEMBER 2012

(AENI JAMILIA)

Perpustakaan Universitas Budi Luhur

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama	:	Aeni Jamilia
Nomor Induk Mahasiswa	:	1011600846
Konsentrasi	:	Teknologi Sistem Infomasi
Jenjang Studi	:	Strata 2
Judul	:	Rancangan Implementasi Protokol S/MIME pada Layanan E-mail Sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi Secara *Online:* Studi Kasus PT. XYZ

Jakarta, 10 Agustus 2012

Tim Penguji: Tanda tangan:

Ketua,
Dr. Moedjiono, M.Sc .....

Anggota,
Dr. Ir. Nazori A.Z., M.T. .....

Anggota,
Hadi Syahrial, M.M., M.Kom. .....

Pembimbing,
Drs. Moedjiono, M.Sc. .....

Pembimbing Pendamping,
Hadi Syahrial, M.M., M.Kom. .....

Ketua Program Studi,

Dr. Ir. Nazori A.Z., M.T.

Perpustakaan Universitas Budi Luhur

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.*

Perpustakaan Universitas Budi Luhur

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. XYZ 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. XYZ 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. XYZ can be met.

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

Perpustakaan Universitas Budi Luhur

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Segala puji dan syukur senantiasa terpanjatkan ke hadirat Allah SWT yang telah memberikan rahmat dan ridho-Nya sehingga penulis dapat menyelesaikan tesis yang berjudul "RANCANGAN IMPLEMENTASI PROTOKOL S/MIME PADA LAYANAN E-MAIL SEBAGAI UPAYA PENINGKATAN JAMINAN KEAMANAN DALAM TRANSAKSI INFORMASI SECARA *ONLINE*: Studi Kasus Pada PT. XYZ". Shalawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu. Dalam penyusunan tesis ini, penulis menyampaikan terima kasih yang setulusnya kepada:

1. Suamiku, Julio Cancero Marsyah Simbolon, yang senantiasa memberikan cinta, semangat dan dukungan penuh. "*You are my soul & inspiration...* "
2. Bapak, ibu, ayah Simbolon dan ibu Ayu tercinta yang senantiasa memberikan kasih sayang, nasihat, dukungan semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
3. Adik-adikku yang selalu memberi warna dan keceriaan.
4. Bapak Dr. Moedjiono, M.Sc., Bapak Dr. Ir. Nazori Az, M.T. dan Bapak Hadi Syahrial, M.M., M.Kom. yang telah banyak memberikan saran dan masukan dalam penyusunan proposal tesis ini.
5. Mbak Be Jhe atas dukungan transportasinya.
6. Mas Sulis, Mbak Ratih, Mbak Reni dan kawan-kawan MKOM UBL 2010.

"Tiada gading yang tak retak". Penulis menyadari penulisan tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun demi tercapainya penulisan yang lebih baik. Saran dan kritik dapat dikirimkan ke alamat e-mail hikaru_89crypt@yahoo.co.id.

Wassalamu'alaikum. Wr. Wb.

Jakarta, Juli 2012

AeNi

Perpustakaan Universitas Budi Luhur

DAFTAR ISI

Halaman

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

DAFTAR GAMBAR

Gambar Halaman

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

DAFTAR TABEL

Perpustakaan Universitas Budi Luhur

DAFTAR LAMPIRAN

Lampiran Halaman

Perpustakaan Universitas Budi Luhur

DAFTAR PUSTAKA

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

[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.

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

[CCS 2008] Anonim. 2008. *DRM Technologies-DRM (Part 2)*. http://cryptocrats.com/. 6 Juni 2012.

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

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

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

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

[GAR 2009] S. Garfinkel. 2009. Signed, *Dealed and Delivered, CSO Online*. www.csonline.com/read/040104 /shop/html/. 1 Juli 2012.

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