

**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**

**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**



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 ijin 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





**PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PENGESAHAN

Nama : Aeni Jamilia
Nomor Induk Mahasiwa : 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:

Ketua,
Dr. Moedjiono, M.Sc

Tanda tangan:

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.

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 penelitian 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*.

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.

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 Syahril, 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

DAFTAR ISI

	Halaman
ABSTRAK	i
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vii
DAFTAR TABEL	ix
DAFTAR LAMPIRAN	x
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Masalah Penelitian	2
1.2.1. Identifikasi Masalah	2
1.2.2. Batasan Masalah	3
1.2.3. Rumusan Masalah	3
1.3. Tujuan dan Manfaat Penelitian	4
1.3.1. Tujuan Penelitian	4
1.3.2. Manfaat Penelitian	4
1.4. Sistematika Penulisan	4
1.5. Daftar Istilah	5
BAB II LANDASAN PEMIKIRAN	6
2.1. Tinjauan Pustaka	6
2.1.1. E-mail	6

2.1.2. Aspek Keamanan Jaringan Komputer	13
2.1.3. <i>E-mail Security</i>	15
2.1.4. Kriptografi.....	18
2.1.4.1. Enkripsi/Dekripsi	18
2.1.4.2. Tanda Tangan Digital	20
2.1.5. Sertifikat Digital.....	21
2.1.6. <i>Public Key Infrastructure (PKI)</i>	24
2.1.7. MIME	26
2.1.8. S/MIME	29
2.2. Tinjauan Studi	33
2.3. Tinjauan Objek Penelitian.....	36
2.3.1. Objek Penelitian.....	36
2.3.2. <i>Hardware</i> yang Akan Digunakan	37
2.3.3. <i>Software</i> yang Akan Digunakan	38
2.4. Kerangka Konsep	39
2.5. Hipotesis Penelitian	40
BAB III RANCANGAN PENELITIAN	41
3.1. Metode Penelitian	41
3.2. Langkah Penelitian	42
3.3. Jadwal Penelitian	45
BAB IV ANALISIS DAN PEMBAHASAN	46
4.1. Gambaran Umum	46
4.2. Infrastruktur E-mail PT. XYZ	47

4.3. Klasifikasi Data/Informasi PT. XYZ	48
4.4. Proses Transaksi Data/Informasi	49
4.5. Model Keamanan	52
4.6. Hambatan/Kendala yang Dihadapi	52
4.7. Pemilihan Protokol S/MIME	52
4.8. Analisa Kebutuhan Implementasi S/MIME	53
4.9. Rancangan Implementasi S/MIME	53
4.10. Pembangunan Implementasi Protokol S/MIME	55
4.11. Simulasi dan Pengujian Keamanan Transaksi E-mail Non Protokol S/MIME	60
4.12. Simulasi dan Pengujian Transaksi E-mail Menggunakan Protokol S/MIME	65
4.13. Hasil Perbandingan Pengujian Keamanan Transaksi E-mail	71
4.14. Analisis Keterkaitan Aspek-Aspek Keamanan Informasi pada S/MIME	71
4.15. Manajemen Protokol S/MIME	75
4.16. Rencana Implementasi Protokol S/MIME	76
4.17. Implikasi Penelitian.....	80
BAB V PENUTUP.....	81
DAFTAR PUSTAKA	83
LAMPIRAN-LAMPIRAN.....	86

DAFTAR GAMBAR

Gambar	Halaman
II.1. Arsitektur protokol pada e-mail	7
II.2. Komponen konseptual sistem e-mail	7
II.3. Contoh e-mail <i>header</i> yang ditetapkan dengan RFC 2822	9
II.4. SMTP mengidentifikasi <i>client</i> dan penerima	10
II.5. Otentikasi dasar dengan POP3	11
II.6. Penggunaan SMTP dan POP3	12
II.7. Diagram proses enkripsi dan dekripsi	18
II.8. Diagram proses enkripsi dan dekripsi algoritma simetrik	19
II.9. Diagram proses enkripsi dan dekripsi algoritma asimetrik	20
II.10. Entitas dalam PKI.....	26
II.11. Proses penandatanganan pesan S/MIME	31
II.12. Proses enkripsi/dekripsi pesan S/MIME	32
II.13. Infrastruktur mail server PT. XYZ	37
II.14. Kerangka konsep penelitian	39
III.1. Langkah penelitian	42
IV.1. Struktur organisasi Departemen IT pada PT. XYZ	46
IV.2. Topologi infrastruktur e-mail PT. XYZ	47
IV.3. Alur diagram kirim/terima e-mail antar <i>user</i> PT. XYZ	50
IV.4. Tampilan <i>user interface</i> pada <i>Mozilla Thunderbird</i>	50
IV.5. Tampilan <i>user interface</i> pengiriman e-mail menggunakan <i>Mozilla</i>	

<i>Thunderbird</i>	51
IV.6. Tampilan <i>user interface</i> menggunakan <i>Mozilla Thunderbird</i> pada sisi penerima e-mail	51
IV.7. Usulan topologi infrastruktur e-mail dengan S/MIME	54
IV.8. Proses <i>set-up</i> protokol S/MIME	56
IV.9. Menonaktifkan protokol S/MIME sebelum transaksi e-mail	60
IV.10. Sukses transaksi e-mail antara Direktorat TI dengan Kadep TI	61
IV.11. Penyadapan transaksi e-mail antara Direktorat TI dengan Kadep TI Sukses	61
IV.12. Mengaktifkan protokol S/MIME sebelum transaksi e-mail	66
IV.13. Sukses transaksi e-mail antara Direktorat TI dengan Kadep TI	66
IV.14. Penyadapan transaksi e-mail antara Direktorat TI dengan Kadep TI Gagal	66
IV.15. Bentuk konten e-mail menggunakan protokol S/MIME	67
IV.16. Format hasil penyadapan pesan S/MIME	72

DAFTAR TABEL

Tabel	Halaman
II.1. Tipe konten S/MIME.....	29
II.2. Studi pustaka	35
III.1. Jadwal penelitian	45
IV.1. <i>Account</i> e-mail untuk simulasi transaksi e-mail	55
IV.2. Korespondensi sertifikat digital dengan <i>account</i> e-mail	57
IV.3. Korespondensi <i>import</i> sertifikat digital dengan <i>account</i> e-mail	58
IV.4. Hasil simulasi transaksi e-mail non S/MIME antar <i>account</i> e-mail	62
IV.5. Hasil pengujian keamanan transaksi e-mail non S/MIME antar <i>account</i> e-mail	63
IV.6. Hasil simulasi transaksi e-mail menggunakan S/MIME antar <i>account</i> e-mail	68
IV.7. Hasil pengujian keamanan transaksi e-mail menggunakan S/MIME antar <i>account</i> e-mail	69
IV.8. <i>Timeline</i> Susunan Rencana Implementasi Protokol S/MIME	79

DAFTAR LAMPIRAN

Lampiran	Halaman
1. Transkrip wawancara awal antara penulis dengan Manajer TI.....	86
2. Transkrip wawancara antara penulis dengan <i>Network and Server Administrator</i> tentang infrastruktur e-mail	88
3. Transkrip wawancara antara penulis dengan <i>Network and Server Administrator</i> tentang transaksi data/informasi	89
4. Transkrip wawancara antara penulis dengan Manajer TI tentang analisis kebutuhan implementasi protokol S/MIME	91
5. Transkrip wawancara antara penulis dengan <i>Network and Server Administrator</i> tentang kebutuhan implementasi S/MIME	92
6. Pembangunan database sertifikat digital	93
7. Pembangkitan CA dan sertifikat digital	94
8. <i>Export</i> file sertifikat digital	97
9. <i>Import</i> file sertifikat digital	99
10. Simulasi dan pengujian implementasi S/MIME pada layanan e-mail	101

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/](http://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.