



**PENERAPAN APLIKASI PENGGABUNGAN TANDATANGAN  
DIGITAL DENGAN TANDATANGAN MANUAL UNTUK  
KEAMANAN BERKAS ELEKTRONIK PADA NISSIN ELECTRIC  
CO LTD**

**SKRIPSI**

**AMINATUZ ZUHRAH**

**1130511041**

**UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA  
FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI TEKNIK INFORMATIKA  
2015**



**PENERAPAN APLIKASI PENGGABUNGAN TANDATANGAN  
DIGITAL DENGAN TANDATANGAN MANUAL UNTUK  
KEAMANAN BERKAS ELEKTRONIK PADA NISSIN ELECTRIC  
CO LTD**

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Meraih Gelar Sarjana**

**AMINATUZ ZUHRAH**

**1130511041**

**UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA  
FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI TEKNIK INFORMATIKA  
2015**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Aminatuz Zuhrah

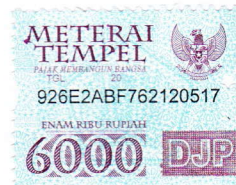
NRP : 1130511041

Tanggal : 31 Juli 2015

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 31 Juli 2015

Yang Menyatakan,



(Aminatuz Zuhrah)

## **PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS**

---

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Aminatuz Zuhrah  
NRP : 1130511041  
Fakultas : Ilmu Komputer  
Program Studi : Teknik Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Rights*) atas karya ilmiah saya yang berjudul: Penerapan Aplikasi Penggabungan Tandatangan Digital Dengan Tandatangan Manual Untuk Keamanan Berkas Elektronik Pada Nissin Electric Co., Ltd.

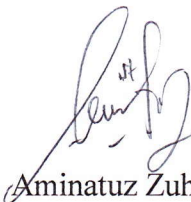
Beserta perangkat yang ada jika diperlukan. Dengan Hak Bebas Royalti ini Universitas Pembanguna Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 31 Juli 2015

Yang Menyatakan,

  
Aminatuz Zuhrah

## PENGESAHAN

Skripsi diajukan oleh:

Nama : Aminatuz Zuhrah  
NRP : 1130511041  
Program Studi : Teknik Informatika  
Judul Skripsi : Penerapan Aplikasi Penggabungan Tandatangan Digital dengan Tandatangan Manual Untuk Keamanan Berkas Elektronik Pada Nissin Electric Co., Ltd.

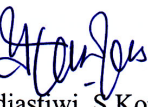
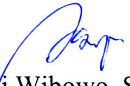
Telah berhasil dipertahankan di hadapan tim penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jakarta



Jayanta, S.Kom., M.Si  
Ketua Penguji



Henki Bayu Seta, S.Kom., M.TI  
Penguji I  
Dr. Nidjo Sandjojo, M.Sc  
Dekan



Prasetyo Adi Wibowo, S.Kom., M.TI  
Penguji II (Pembimbing)  
Yuni Widiastiwi, S.Kom., M.Si  
Ka. Prodi

Ditetapkan di : Jakarta

Tanggal Ujian : 31 Juli 2015

# PENERAPAN APLIKASI PENGGABUNGAN TANDA TANGAN DIGITAL DENGAN TANDA TANGAN MANUAL UNTUK KEAMANAN BERKAS ELEKTRONIK PADA NISSIN ELECTRIC CO., LTD.

Aminatuz Zuhrah

## Abstrak

Pengiriman dokumen melalui e-mail sudah merupakan hal komersial. Pengamanan dokumen untuk menjaga keotentikannya sampai di pihak penerima dalam perjalanan di jaringan relative tidak aman salah satunya dengan cara memberi tandatangan digital. Salah satu metode untuk membuat tandatangan digital adalah tandatangan manual yang dikombinasikan dengan DSA (*Digital Signature Algorithm*). Tujuan dari penelitian ini adalah mengamankan e-dokumen dengan metode penggabungan penggabungan tanda tangan manual dan DSA (*Digital Signature Algorithm*) sebagai salah satu solusi pada masalah manajemen kunci dan memenuhi kebutuhan ketidaktunggalan penandatanganan yang dalam penelitian ini disebut *signer*. Biometrik yang digunakan adalah tandatangan manual/ *offline*. Pada penelitian ini keluaran yang dihasilkan adalah berupa Aplikasi Kriptografi dengan tiga tahap proses inti (Pembangkitan Kunci, Pembuatan tandatangan digital, dan verifikasi). Selanjutnya e-dokumen, tandatangan *digital* dan kunci publik ditransmisikan melalui internet via *e-mail* pada pihak penerima yang selanjutnya dalam penelitian ini disebut *verifier*. Kemudian pihak *verifier* memverifikasi apakah hasilnya valid yaitu e-dokumen tersebut masih otentik dan pengirim adalah *penandatanganan yang sah* sebenarnya dari e-dokumen tersebut. Sebaliknya jika hasilnya tidak valid yaitu. E-dokumen tersebut sudah tidak otentik dan atau pengirim bukanlah *signer* sebenarnya dari e-dokumen tersebut.

**Kata Kunci:** *Signer, verifier, Tandatangan off-line, Tandatangan digital, DSA (Digital Signature Algorithm).*

# **APPLICATION OF INTEGRATION BETWEEN OFFLINE SIGNATURE AND DIGITAL SIGNATURE FOR E-DOCUMENT SECURITY AT NISSIN ELECTRIC CO., LTD.**

**Aminatuz Zuhrah**

## **Abstract**

Document transmission through email has been used as a commercial transaction. One of the method to keep the document authentic while it's transmit through insecure network is with embed digital signature. One of method to create digital signature is with merger between offline signatures with digital signature algorithm. . The purpose of this research is to create cryptographic applications with merger offline signatures and DSA (Digital Signature Algorithm) as one of the solution to the problem of management key and meet the needs nonsingular of signer. In this research as an input (key generator) are offline signature with one or more users that able to generate one or more digital signatures for one e-document. Furthermore, e-documents, digital signatures and public key is transmitted over the Internet via e-mail to the verifier. Afterwards the verifier verifies whether its result is valid which means the e-documents are still authentic and the sender is the authorized signer of the e-document. Conversely, if the result is not valid that means the e-document is not authentic and signer is not the authorized sender of the e-document.

**Keywords:** Signer, Verifier, offline signature, Digital signature, DSA (Digital Signature Algorithm).

## **KATA PENGANTAR**

Puji dan syukur penulis panjatkan atas kehadiran ALLAH SWT atas segala karunia-Nya sehingga skripsi ini berhasil diselesaikan. Judul yang dipilih dalam penelitian ini yang dilaksanakan sejak Februari 2015 adalah Penerapan Aplikasi Penggabungan Tandatangan Digital Dengan Tandatangan Manual Untuk Keamanan Berkas Elektronik Pada Nissin Electric Co., Ltd. Terimakasih penulis ucapkan kepada bapak Prasetyo Adi Wibowo selaku dosen pembimbing, ibu Yuni Widiastiwi selaku kepala Program Studi, Bapak Jayanta Selaku pembimbing akademik serta Bapak Nidjo Sanjojo selaku dekan yang telah memberikan nasihat, saran, bimbingan serta kebijakan yang tentunya sangat bermanfaat bagi penulis.

Disamping itu, ucapan terima kasih juga disampaikan kepada ayahanda dan ibunda tercinta H. Sahmun dan Hj. Ruqiah Ulfa, kakak dan adik tersayang Riza Noviana Ulfa dan Multazam Aulawi serta seluruh keluarga yang tidak henti-hentinya memberikan penulis semangat dan doa. Penulis juga sampaikan terima kasih kepada teman-teman kelas regular G yang telah membantu dan mendukung terus dalam penulisan skripsi ini.

Jakarta, 31 Juli 2015

Aminatuz Zuhrah



## DAFTAR ISI

HALAMAN JUDUL.....	i
PERNYATAAN ORISINALITAS .....	ii
PERNYATAAN PERSETUJUAN PUBLIKASI .....	iii
PENGESAHAN .....	iv
ABSTRAK .....	v
ABSTRACT .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR .....	xi
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN .....	1
I.1 Latar Belakang.....	1
I.2 Perumusan Masalah .....	3
I.3 Batasan Masalah .....	3
I.4 Tujuan Penelitian .....	3
I.5 Manfaat Penelitian .....	3
I.6 Sistematika Penulisan.....	3
BAB II LANDASAN TEORI .....	5
II.1 Tinjauan Pustaka .....	5
II.2 Landasan Teori .....	7
II.3 Komparasi Dengan Penelitian Terdahulu.....	22
BAB III METODE PENELITIAN.....	24
III.1 Bahan Penelitian.....	24
III.2 Alat Penelitian.....	25
III.3 Alur Penelitian .....	25
III.4 Model Pengembangan Sistem dengan Metode Waterfall .....	26
III.5 UML .....	29
III.6 Flowchart.....	31
BAB IV PERANCANGAN DAN IMPLEMENTASI .....	35
IV.1 Perancangan Umum Aplikasi .....	35
IV.2 Implementasi.....	38
BAB V KESIMPULAN DAN SARAN.....	61
V.1 Kesimpulan .....	61
V.2 Saran.....	62

DAFTAR PUSTAKA .....63

RIWAYAT HIDUP

LAMPIRAN

## DAFTAR TABEL

Tabel 1 Komparasi Penelitian Dengan Yang Sebelumnya.....	22
Tabel 2 Daftar E-doc yang di gunakan.....	44
Tabel 3 Rekapitulasi Hasil Verifikasi kasus 1-7 .....	58

## DAFTAR GAMBAR

Gambar 1 Komponen Usecase Diagram .....	19
Gambar 2 Simbol Kelas Diagram .....	20
Gambar 3 Simbol Sequence Diagram .....	21
Gambar 4 Alur proses Aplikasi .....	25
Gambar 5 Tahapan Pengembangan Sistem Dengan Metode waterfall .....	26
Gambar 6 Usecase Diagram Aplikasi.....	29
Gambar 7 Sequence Diagram Menandatangani dokumen .....	30
Gambar 8 Sequence Diagram Membuat Kunci.....	30
Gambar 9 Sequence Diagram Membuat Tandatangan Digital.....	31
Gambar 10 Sequence Diagram Memverifikasi Dokumen.....	31
Gambar 11 Create Key Flowchart.....	32
Gambar 12 Signing Flowchart.....	33
Gambar 13 Verify Flowchart.....	34
Gambar 14 Perancangan Antar Muka Program utama.....	35
Gambar 15 Perancangan Antar Muka Membuat Sepasang Kunci .....	36
Gambar 16 Perancangan Antar Muka Membangkitkan Tandatangan Digital .....	36
Gambar 17 Perancangan Antar Muka Verifikasi .....	37
Gambar 18 Menu utama .....	38
Gambar 19 Generate Key .....	39
Gambar 20 Generate Signature .....	39
Gambar 21 Verifikasi .....	40
Gambar 22 Pembangkitan Sepasang Kunci Dengan Tandatangan andinttd .....	41
Gambar 23 Tampilan Parameter DSA.....	42
Gambar 24 Tampilan Kunci Pivate .....	42
Gambar 25 Tampilan Kunci Publik.....	43
Gambar 26 Tampilan Hasil Tandatangan Digital dari Abstrak.pdf .....	43
Gambar 27 Tampilan Hasil Tandatangan Digital dari Kriptografi.docx.....	44
Gambar 28 Jenis Dokumen Yang bisa di tandatangi.....	44
Gambar 29 Ukuran File .Sig.....	44
Gambar 30 Tampilan Email yang Diterima Verifier dari Signer .....	46
Gambar 31 Tampilan Muka file Abstrak.pdf yang diunduh Verifier.....	47
Gambar 32 Tampilan Kunci Public yang diunduh Verifier .....	48
Gambar 33 Tampilan Tandatangan Digital Sah yang Diunduh Verifier .....	48
Gambar 34 Hasil verifikasi dari lampiran yang telah diunduh.....	48
Gambar 35 Kunci Publik Yang Tidak Sah.....	49
Gambar 36 Hasil Verifikasi Kasus 2 .....	49
Gambar 37 Perbandingan Output dari Potongan (a) Gambar 34 dan (b) dari Potongan Gambar 36 .....	50
Gambar 38 Hasil verifikasi Kasus 3 .....	51
Gambar 39 Perbandingan Potongan Output dari (a) Gambar 34 dan (b) .....	51
Gambar 40 Hasil Verifikasi kasus 4.....	52

Gambar 41 Perbandingan Keluaran dari (a) Potongan Gambar 34 dan (b) Potongan Gambar 40 .....	53
Gambar 42 Hasil Verifikasi kasus 5 .....	54
Gambar 43 Perbandingan Keluaran dari (a) Potongan Gambar 34 dan (b) Potongan Gambar 42 .....	54
Gambar 44 Hasil Verifikasi Kasus 6 .....	55
Gambar 45 Perbandingan Keluaran dari (a) Potongan Gambar 34 dan (b) Potongan Gambar 44 .....	56
Gambar 46 Hasil Verifikasi Kasus 7 .....	57
Gambar 47 Perbandingan Keluaran dari (a) Potongan Gambar 34 dan (b) Potongan Gambar 46 .....	57

## **DAFTAR LAMPIRAN**

Lampiran 1 Kode Program  
Lampiran 2 Hasil Verifikasi