

**ANALISIS DAN PENGEMBANGAN APLIKASI
PELAPORAN MODUL PENERIMAAN NEGARA
GENERASI 2 (MPN G-2) MENGGUNAKAN
DIGITAL SIGNATURE
PADA PT. BANK BNI SYARIAH**

TESIS



Oleh :
AHMAD MUHARRIA RAJHASLA PUTRA
1311600207

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

JAKARTA
2016

**ANALISIS DAN PENGEMBANGAN APLIKASI
PELAPORAN MODUL PENERIMAAN NEGARA
GENERASI 2 (MPN G-2) MENGGUNAKAN
DIGITAL SIGNATURE
PADA PT. BANK BNI SYARIAH**

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelar Magister Ilmu Komputer (MKom)



Oleh :

AHMAD MUHARRIA RAJHASLA PUTRA

1311600207

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

**JAKARTA
2016**



PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDILUHUR

LEMBAR PENGESAHAN

Nama : AHMAD MUHARRIA RAJHASLA PUTRA
Nomor Induk Mahasiswa : 1311600207
Konsentrasi : Teknologi Sistem Informasi
Jenjang Studi : Strata 2
Judul : Analisis dan Pengembangan Aplikasi Pelaporan
Modul Penerimaan Negara Generasi 2 (MPN G-2)
Menggunakan Digital Signature pada PT. Bank BNI
Syariah

Jakarta, 22 Februari 2016

Tim Penguji :

Tandatangan :

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

Anggota,
Dr. Ir. Nazori AZ, MT

Pembimbing,
Dr. Ir. Wendi Usino, M.Sc, MM

Ketua Program Studi

Dr. Ir. Nazori AZ, MT



**PROGRAM STUDI :MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDILUHUR**

LEMBAR PERNYATAAN

Nama : AHMAD MUHARRIA RAJHASLA PUTRA
NIM : 1311600207
Program Studi : MAGISTER ILMU KOMPUTER
Fakultas : PASCA SARJANA

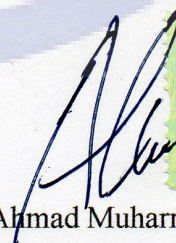
Menyatakan bahwa TESIS yang berjudul :

Analisis dan Pengembangan Aplikasi Pelaporan Modul Penerimaan Negara
Generasi 2 (MPN G-2) Menggunakan Digital Signature pada PT. Bank BNI
Syariah

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 apabila dikemudian pernyataan ini tidak benar.

Jakarta, 22 Februari 2016


(Ahmad Muharria Rajhasla Putra)



ABSTRAK

Sebagai salah satu bank persepsi, Bank BNI Syariah berkewajiban selain mengembangkan sistem pembayarannya juga diharuskan untuk menyampaikan laporan ke Kementerian Keuangan. Ada 2 laporan yang harus disampaikan. Yaitu Laporan pada H+0 dan Laporan pada H+1. Laporan pada H+0 terdiri dari Laporan DNP (Daftar Nominatif Penerimaan) dan LHP (Laporan Harian Penerimaan). Kedua Laporan tersebut harus disampaikan dalam format text file. Laporan pada H+1 yaitu laporan Bank Statement (BS) atau laporan rekening koran yang berisi transaksi berdasarkan sistem bank yang disertai dengan *digital signature*. Penelitian ini memaparkan mengenai pengembangan aplikasi pelaporan MPN G-2 pada divisi operasional di PT. BNI Syariah menggunakan *digital signature* dengan algoritma RSA. Hasil dari penelitian ini adalah aplikasi dapat menghasilkan laporan sebelum jam 09.00 H+1 sehingga dapat mencegah terjadinya sanksi denda. Untuk proses otentikasi data dapat diimplementasikan dengan algoritma RSA sehingga data rekening koran menjadi valid.

Kata Kunci : Pelaporan, digital signature, RSA, rekening koran, otentikasi

ABSTRACT

As one of the bank of perception, BNI Syariah has a duty not only to develop the payment system but also to require submitting a report to the Ministry of Finance. There are two things to be reported, namely the report on $H + 0$ and report on $H + 1$. Report on $H + 0$ consists of DNP Reports (Daftar Nominatif Penerimaan) and LHP (Laporan Harian Penerimaan). Both reports should be submitted in text file format. Report on $H + 1$ is report of Bank Statement (BS) or Rekening Koran report that contains transaction based on bank systems. This research describes about development MPN G-2 reporting at PT. BNI Syariah by implementing digital signature with RSA algorithm. The result of this research is the application generates the reporting before 09.00 $H+1$ and not have penalty. For data authentication, this application implement RSA algorithm, so data of rekening koran will be valid.

Key Note: Reporting, digital signature, RSA, Rekening Koran, authentication

KATA PENGANTAR

Alhamdulillahirabbil ‘aalamin, puji dan syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan limpahan rahmat dan anugerah-Nya kepada kita semua.

Shalawat teriring salam semoga senantiasa terlimpah kepada Baginda Nabi Muhammad SAW, keluarganya, sahabat serta pengikutnya sampai akhir zaman.

Alhamdulillah penulis dapat menyelesaikan tesis ini sebagai salah satu syarat untuk mendapatkan gelar Magister Ilmu Komputer (MKOM).

Penulis menyadari sepenuhnya akan kekurangan serta kekhilafan atas penulisan tesis ini, karenanya tesis ini jauh dari sempurna. Namun penulis berharap penulisan tesis ini dapat memenuhi salah satu syarat meraih gelar Magister Ilmu Komputer dan semoga tesis ini dapat memberikan manfaat bagi penulis khususnya dan umumnya para pembaca.

Dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah memberikan bantuan atas penyelesaian penulisan tesis ini, dengan segala kerendahan hati, rasa terima kasih ini penulis ucapkan terutama kepada yang terhormat :

1. Prof. Ir. Suryo Hapsoro Tri Utomo, PhD sebagai Rektor Universitas Budi Luhur.
2. Prof. Dr. Moedjiono, M.Sc sebagai Direktur Program Pascasarjana Universitas Budi Luhur
3. Dr. Ir. Wendi Usino, M.Sc sebagai pembimbing yang telah banyak meluangkan waktu, tenaga dan masukannya. Semoga Allah SWT membalas-Nya dengan pahala yang berlimpah. Amin
4. Dr. Ir. Nazori AZ, MT sebagai Kaprodi Magister Ilmu Komputer Universitas Budi Luhur.
5. Seluruh dosen, staff, dan karyawan Universitas Budi Luhur yang telah memberikan bantuannya.

6. Orangtua, istri, anak dan keluarga yang telah banyak memotivasi, mendoakan untuk kesuksesan.
7. Teman-teman seangkatan yang telah sama-sama berjuang.
8. Karyawan-karyawan PT. Bank BNI Syariah
9. Teman-teman asrama mahasiswa Aceh FOBA yang telah banyak membantu.

Kiranya budi baik yang diberikan kepada penulis Insya Allah akan mendapatkan balasan dari Allah SWT.

Akhirnya untuk penyempurnaan tesis ini penulis mengharapkan masukan dan saran-saran yang bersifat membangun.

Jakarta, 22 Februari 2016

Penulis



DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
DAFTAR LAMPIRAN	xii
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Masalah Penelitian	3
1.2.1 Identifikasi Masalah	3
1.2.2 Pembatasan Masalah	4
1.2.3 Rumusan Masalah	4
1.3 Tujuan dan Manfaat penelitian	5
1.4 Tata Urut Penulisan	5
BAB II LANDASAN TEORI DAN KERANGKA KONSEP	
2.1 Tinjauan Pustaka	6
2.1.1 Kriptografi.....	6
2.1.1.1 Tujuan Kriptografi.....	6
2.1.1.2 Teknik Kriptografi.....	7
2.1.2 Algoritma RSA.....	9

2.1.2.1 Proses Pembangkitan Kunci.....	10
2.1.2.2 Proses Enkripsi.....	10
2.1.2.3 Proses Dekripsi.....	11
2.1.3 Pembangkit Bilangan Prima.....	12
2.1.3.1 Proses Algoritma The Sieve Of Eratosthenes.....	12
2.1.4 Fungsi Hash Satu Arah.....	15
2.1.5 Tanda Tangan Digital (Digital Signature).....	16
2.1.5.1 Pemberian Tanda Tangan Digital.....	16
2.1.5.2 Verifikasi Tanda Tangan Digital.....	17
2.1.6 XML.....	17
2.1.7 Web Service	18
2.1.8 SOAP	18
2.1.9 Kualitas Perangkat Lunak.....	20
2.1.10 Pengujian Perangkat Lunak	20
2.2 Tinjauan Studi	21
2.3 Tinjauan Obyek Penelitian	24
2.4 Kerangka Konsep	27
2.5 Hipotesis	29

BAB III METODOLOGI DAN RANCANGAN PENELITIAN

3.1 Tempat Penelitian	30
3.2 Metode Pengumpulan Data	30
3.3 Tahapan Penelitian.....	30
3.4 Teknik Pengujian Sistem	32

3.5 Jadwal Penelitian	32
-----------------------------	----

BAB IV ANALISIS, PENGEMBANGAN APLIKASI , DAN IMPLIKASI PENELITIAN

4.1 Manajemen Aplikasi Pelaporan dan Kebutuhan Aplikasi.....	34
4.1.1 Aplikasi Pelaporan MPN G-2.....	34
4.1.2 Fungsi Aplikasi Pelaporan MPN G-2.....	34
4.2 Analisis.....	43
4.2.1 Analisis Pelaporan MPN G-2	35
4.2.2 Analisis Proses Bisnis.....	35
4.2.3 Analisis kebutuhan Fungsional dan Non Fungsional.....	39
4.2.4 Analisis Pengguna.....	40
4.2.5 Analisis Sistem.....	41
4.3 Perancangan Teknik Kriptografi dan Tanda Tangan Digital.....	51
4.4 Implementasi Aplikasi Pelaporan MPN G-2	54
4.5 Pengujian Sistem	57
4.7 Implikasi Penelitian.....	68
4.9.1 Aspek Sistem.....	69
4.9.2 Aspek Manajerial.....	70
4.9.3 Aspek Penelitian Lanjut.....	70
4.10 Rencana Implementasi.....	71

BAB V PENUTUP.....	73
--------------------	----

DAFTAR PUSTAKA.....	74
---------------------	----

LAMPIRAN-LAMPIRAN.....	76
------------------------	----



DAFTAR GAMBAR

Gambar	Halaman
II-1 Alur Kriptografi Kunci Simetris.....	8
II-2 Alur Kriptografi Kunci Asimetris	9
II-3 Ilustrasi Tanda Tangan Digital	16
II-4 Pola Pikir Pemecahan Masalah	27
II-5 Kerangka Pemikiran data Rekening Koran.....	28
III-1 Tahapan Penelitian.....	31
IV-1 Alur proses pembuatan laporan MPN G-2.....	35
IV-2 Detail Alur proses pelaporan MPN G-2.....	36
IV-3 Detail Perbaikan Bisnis Proses pada Sistem Pelaporan MPN G-2	37
IV-4 Actor Sistem Aplikasi Pelaporan MPN G-2.....	41
IV-5 Uses Cases Admin User aplikasi pelaporan MPN G-2.....	42
IV-6 Uses Cases Pegawai divisi Operasional.....	43
IV-7 Activity Diagram Pendaftaran User Akses Oleh Admin User.....	44
IV-8 Activity Diagram Pengguna Login	45
IV-9 Activity Diagram Pegawai Divisi Operasional untuk <i>download</i>	46
IV-10 Sequence Diagram Pendaftaran User.....	48
IV-11 Sequence Diagram Login Pengguna ke Aplikasi	49
IV-12 Sequence Diagram Download.....	50
IV-13 Ilustrasi teknik kriptografi dan tanda tangan digital.....	53

IV-14 Tampilan Awal Log in Aplikasi.....	55
IV-15 Halaman Utama Aplikasi Pelaporan MPN G-2	56
IV-16 Hasil Pengujian Fungsionalitas Proses create pelimpahan	59
IV-17 Hasil Pengujian Fungsionalitas Proses Konfirmasi Masukan data nomor sakti.....	60
IV-18 Informasi Transaksi secara real time.....	61
IV-19 Hasil Informasi dari aplikasi mengenai respon informasi create pelimpahan/nomor sakti yang kosong.....	62
IV-20 Hasil Informasi dari aplikasi mengenai respon informasi create pelimpahan yang sudah tersedia sebelumnya.....	63
IV-21 Test Case pada Form Login Aplikasi dengan user yang tidak memiliki otoritas.....	64
IV-22 Tampilan untuk download file laporan H+1 pada aplikasi MPN G-2.....	65
IV-23 Digital Signature pada file xml laporan rekening koran	66
IV-24 Data transaksi yang sudah dihasilkan ke dalam file laporan rekening koran	66
IV-25 Test Case pada aplikasi simulator upload rekening koran.....	68
IV-26 Test Case pada aplikasi simulator hasil autentikasi laporan rekening koran	68

DAFTAR TABEL

Table	Halaman
II-1 Tinjauan Studi Pembahasan Penelitian Sejenis.....	23
II-2 Spesifikasi Pendukung Software dan hardware	26
III-1 Jadwal Penelitian	32
IV-1 Tingkatan Pengguna dan Hak Akses Pengguna	40
IV-2 Spesifikasi Pengembangan Laporan	54
IV-3 Pengujian Fungsional Indikator Suitability (Create pelimpahan)	58
IV-4 Pengujian Fungsional Indikator Suitability (Respon dari sistem)	59
IV-5 Pengujian Fungsional Indikator Suitability (Rekapan Laporan)	60
IV-6 Tabel Pengujian Fungsional Indikator Accuracy (Validasi Informasi Form Input Nomor Sakti pada Sistem)	61
IV-7 Pengujian Fungsional Indikator Security	63
IV-8 Pengujian Fungsional Indikator Compliance	64
IV-9 Penjelasan Pengembangan Penelitian lanjut	71
IV-10 Rencana Implementasi	71

DAFTAR LAMPIRAN

Lampiran	Halaman
1 Lampiran User Acceptance Test (UAT)	77
2 Lampiran Transkrip Wawancara	80



DAFTAR PUSTAKA

- [Azmi 2010] Azmi, Meri, dan Dwi Sudarno Putra, *Implementasi Teknologi XML Dalam Pertukaran Data Antar Server* (Studi di Dinas Pendidikan dan Pengajaran Kota Yogyakarta) ISSN : 1858-3709, Poli Rekayasa Vol 6, No. 1, pp.58-70, Padang, 2010.
- [BERN 2005] Renaldy,B,. 2005. “*Implementasi XML Signature pada Dokumen XML untuk Transkrip Nilai Online*. Jurnal Informatika UKM, Vol. I, No. 2, Desember 2005: 107 – 120
- [Caroline 2010] Caroline, Maureen Linda. *Perbandingan Algoritma Kriptografi Kunci Publik RSA, Rabin, dan Elgamal*, Makalah Teknik Informatika, Bandung, 2010.
- [Dafid 2006] Dafid. Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton, Jurnal Ilmiah STMIK MDP, Vol 2, No 3, pp 20-27, 2006.
- [Hartono 2004] Hartono, Budi. *Ruang Lingkup Kriptografi Untuk Mengamankan Data*, Dinamika Informatika ISSN : 0854-9524, Vol.IX, No.2, pp.1-7, 2004.
- [JAN 2010] Simarmata, Janner. *Rekayasa Perangkat Lunak*, CV ANDI Offset, Yogyakarta, 2010.
- [Laksito 2013] Laksito, Arif Dwi, *Sinkronisasi Jadwal Perkuliahan pada Aplikasi Android menggunakan Teknologi XML-RPC (Studi Kasus di STMIK AMIKOM Yogyakarta)*, Seminar Nasional Teknologi Informasi (SNATI) ISSN : 1907-5022, pp. 1-5, Yogyakarta, 2013.
- [Listiyono 2009] Listiyono, Hersatoto. *Implementasi Algoritma Kunci Publik Pada Algoritma RSA*, Dinamika Infortmatika ISSN : 2085-3343, Vol. I, No.2, pp.95-99, 2009.
- [Lubis 2013] Lubis, Muhammad Safri, et.al., *Penggunaan Algoritma RSA dengan Metode The Sieve of Eratosthenes Dalam Enkripsi dan Deskripsi Pengiriman Email*, Seminar Nasional Aplikasi Teknologi Informasi (SNATI) ISSN : 1907-5022, Yogyakarta, pp. 23-28, 2013.