

**IMPLEMENTASI SMART CARD PADA
SISTEM INFORMASI TRANSAKSI PRABAYAR
(CLIENT SIDE)**

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Teknik Informatika

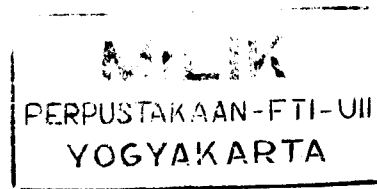


No.	512/A/S/FT-10-11/04
Tanggal	30 Sep 04.
Asal	FAK. TEK. 100574 - UII
Harga	Asip =
FAK. TEK. 100574 - UII UNIVERSITAS ISLAM INDONESIA YOGYAKARTA	

Oleh

Nama : Aljas Kamalfasha
No. Mahasiswa : 00523045

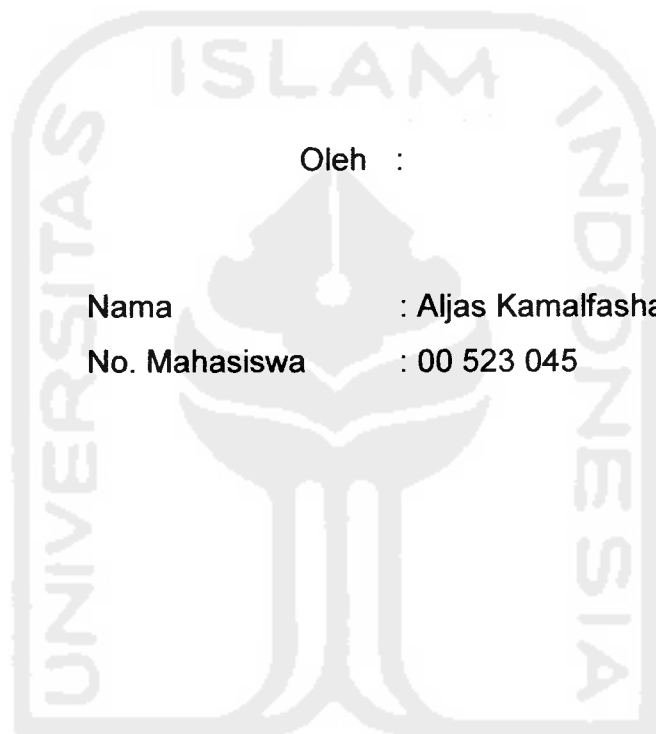
**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
JOGJAKARTA
2004**



LEMBAR PENGESAHAN PEMBIMBING

IMPLEMENTASI *SMART CARD* PADA SISTEM INFORMASI TRANSAKSI PRABAYAR (*CLIENT SIDE*)

TUGAS AKHIR



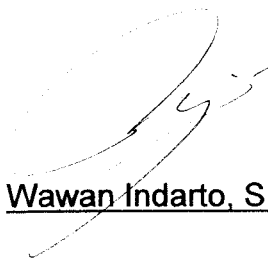
Oleh :

Nama : Aljas Kamalfasha

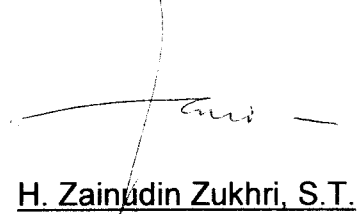
No. Mahasiswa : 00 523 045

Jogjakarta, 4 November 2004

Pembimbing Pelaksana


Wawan Indarto, S.T.

Pembimbing Payung


H. Zainudin Zuhri, S.T.

LEMBAR PENGESAHAN PENGUJI
IMPLEMENTASI SMART CARD PADA
SISTEM INFORMASI TRANSAKSI PRABAYAR
(CLIENT SIDE)

TUGAS AKHIR

Oleh :

Nama : Aljas Kamalfasha
No. Mahasiswa : 00523045

Telah Dipertahankan di Depan Sidang Penguji Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik Informatika
Fakultas Teknologi Industri
Universitas Islam Indonesia

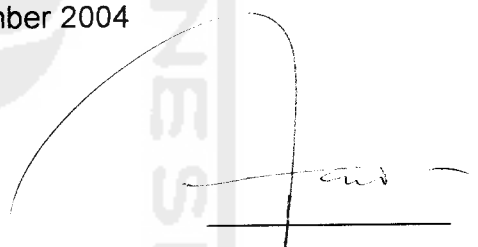
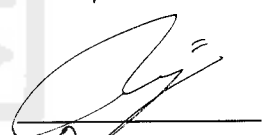
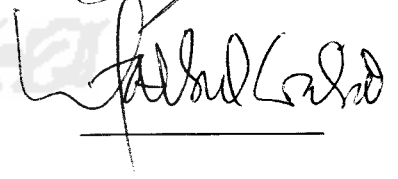
Jogjakarta, 3 November 2004

Tim Penguji

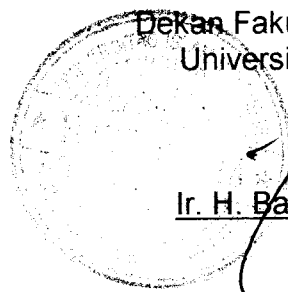
H. Zainudin Zukhri, ST

Wawan Indarto, ST

Fathul Wahid, ST., MSc



Mengetahui,
Dekan Fakultas Teknologi Industri
Universitas Islam Indonesia



Ir. H. Bachrun Sutrisno M.sc

HALAMAN MOTTO

“ Jangan pernah hanya menunggu keberuntungan datang, tetapi paksalah
keberuntungan itu datang “

(*Aljas Kamalfasha*)

“ Akulah si penentu. Aku bisa memilih, melampaui segala rintangan di
depanku atau tersesat dalam keruwetan itu. Semuanya pilihanku, tanggung
jawabku, menang atau kalah, akulah kunci bagi takdirku “

(*Elaine Maxwell*)

“ Pertama – tama, katakan pada dirimu apa yang akan kau raih, lalu lakukan
apa yang perlu kau lakukan “

(*Epictetus*)

“ Pengetahuan adalah Cinta, Cahaya dan Visi “

(*Hellen Keller*)

“ Bersikap jujur adalah yang terbaik “

(*Benjamin Franklin*)

HALAMAN PERSEMBAHAN

Tugas akhir ini saya persembahkan kepada kedua orang tua saya tercinta, InsyaAllah sebagai kado hari ulang tahun saya pada tanggal 25 desember 2004, terima kasih telah terus menerus memberikan hal terbaik untuk masadepan saya, berupa rencana, bimbingan, dukungan, kepercayaan, dan doa yang selalu menjadi pendorong utama saya untuk menjadi lebih baik dan dapat menyelesaikan tugas akhir ini dengan baik.

Aljas Ulva Nadia, *you are the most valuables thing in my life*, Syarifah Aljas Sylvia Abdullah dan Aljas Hammar Abdullah terima kasih sudah menjadi petunjuk arah dalam hidupku.

Almamaterku Universitas Islam Indonesia yang telah menempa dan memberikan saya ilmu pengetahuan, wawasan selama menempuh pendidikan

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Alhamdulillahirabbil'alamin penulis panjatkan kehadiran Allah SWT yang selalu melimpahkan rahmat dan hidayah-Nya sehingga tugas akhir ini dapat penulis selesaikan sesuai dengan waktu yang direncanakan.

Tugas akhir yang berjudul IMPLEMENTASI *SMART CARD* PADA SISTEM INFORMASI TRANSAKSI PRABAYAR (*CLIENT SIDE*) ini disusun sebagai salah satu syarat dalam memperoleh gelar Sarjana Teknik Informatika di Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.

Pada kesempatan ini penulis tidak lupa untuk mengucapkan banyak terima kasih terhadap semua pihak yang telah memberikan dukungan, baik moril maupun materiil. Pihak yang penulis maksud antara lain adalah :
Tidak lupa penulis ucapkan terimakasih yang sebesar-besarnya kepada :

1. Bapak Dr. Ir. H. Luthfi Hasan, M. Sc, selaku Rektor Universitas Islam Indonesia.
2. Bapak Ir. H. Bachrun Sutrisno, M.Sc selaku Dekan Fakultas Teknologi Industri, Universitas Islam Indonesia.
3. Ibu Sri Kusumadewi S.Si, MT, selaku ketua Jurusan Teknik Informatika Universitas Islam Indonesia.

4. Bapak Wawan Indarto, S.T, selaku dosen pembimbing pelaksana yang telah memberikan pengarahan dan saran penyusunan tugas akhir ini.
5. Bapak H. Zainudin Zukhri, S.T, selaku dosen pembimbing payung.
6. Kepada semua pihak yang telah membantu sehingga tugas akhir ini dapat diselesaikan dengan baik.

Penulis menyadari bahwa laporan tugas akhir ini masih mengandung banyak kekurangan karena kesempurnaan itu hanya milik Allah SWT, untuk itu penulis sangat mengharapkan kritik dan sarannya.

Harapan besar penulis, agar karya yang sangat sederhana ini dapat menjadi sumbangan yang berarti bagi kampus tercinta FTI UII Jogja.

Wassalamu'alaikum Wr.Wb.

Jogjakarta, 4 November 2004

Penulis

DAFTAR ISI

Halaman Judul.....	i
Halaman Pengesahan Pembimbing.....	ii
Halaman Pengesahan Penguji.....	iii
Halaman Motto.....	iv
Halaman Persembahan.....	v
Kata Pengantar.....	vi
Daftar Isi	viii
Daftar Tabel.....	xi
Daftar Gambar.....	xii
Abstraksi.....	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	6
1.5 Manfaat Penelitian.....	7
1.6 Metodologi Penelitian.....	7
1.6.1 Metode Pengumpulan Data.....	7
1.6.1.1 Data Primer.....	7
1.6.1.2 Data Sekunder	8
1.6.2 Metode Pengembangan Sistem	8
1.6.2.1 Analisis Kebutuhan	8
1.6.2.2 Perancangan Sistem	8
1.6.2.3 Implementasi Sistem	9
1.6.2.4 Analisis Kerja Perangkat Lunak.....	9
1.7 Sistematika Penulisan	9
BAB II LANDASAN TEORI	12
2.1 Sistem	12
2.2 Informasi	12
2.3 Sistem Informasi	13
2.4 <i>Smart Card</i>	14

2.4.1 Standarisasi <i>Smart Card</i>	14
2.4.2 Jenis <i>Smart Card</i>	18
2.4.3 Jenis Memori Pada <i>Smart Card</i>	20
2.4.4 Komunikasi Pada <i>Smart Card</i>	20
2.5 <i>Smart Card Reader / Writer</i>	21
2.6 Aplikasi Berbasis <i>Smart Card</i>	21
2.7 Kriptografi.....	22
2.7.1 Kunci Simetris.....	23
2.7.2 DES (<i>Data Encryption Standard</i>).....	24
2.7.3 Algoritma DES.....	25
2.8 <i>Programmable Security Code</i> (PSC).....	33
2.9 <i>Random Key Generator</i>	34
2.10 <i>Protection Byte</i>	34
2.11 Algoritma Anti Duplikasi Kartu.....	35
2.12 Teknik Perancangan Sistem.....	37
2.12.1 Diagram Konteks (<i>Context Diagram</i>).....	37
BAB III ANALISIS KEBUTUHAN PERANGKAT LUNAK.....	39
3.1 Metode Analisis.....	39
3.2 Hasil Analisis.....	40
3.2.1 Analisis Kebutuhan Masukan.....	40
3.2.2 Analisis Kebutuhan Keluaran.....	41
3.2.3 Analisis Kebutuhan Antarmuka.....	42
3.2.4 Analisis Kebutuhan Perangkat Lunak.....	42
BAB IV PERANCANGAN PERANGKAT LUNAK.....	43
4.1 Metode Perancangan	43
4.2 Hasil Perancangan.....	43
4.2.1 Struktur Pohon Proses.....	43
4.2.2 Diagram Arus Data (<i>Data Flow Diagram</i>).....	44
4.2.2.1 Diagram Konteks.....	44
4.2.2.2 Diagram Aliran Data Level 1.....	45
4.2.2.3 Diagram Aliran Data Level 2 dari Proses 1.....	47
4.2.2.4 Diagram Aliran Data Level 2 dari Proses 2.....	48
4.2.3 Spesifikasi Proses.....	49
4.2.4 Kamus Data.....	60

4.2.5 Aturan Pengkodean.....	64
4.2.6 Pengalamatan Memori <i>Smart Card</i>	65
4.2.7 Rancangan Kebutuhan Antarmuka (<i>Interface</i>).....	68
BAB V IMPLEMENTASI PERANGKAT LUNAK.....	77
5.1 Batasan Implementasi.....	77
5.2 Implementasi Perangkat Lunak.....	78
5.2.1 Halaman Utama Sistem Informasi Transaksi Prabayar.....	78
5.2.2 Halaman Konfigurasi Jaringan.....	79
5.2.3 Halaman Login.....	80
5.2.4 Halaman Pengaturan Operator.....	81
5.2.5 Halaman Pengaturan Barang.....	83
5.2.6 Halaman Pengaturan Suplier.....	84
5.2.7 Halaman Personalisasi Pelanggan.....	85
5.2.8 Halaman Penjualan.....	86
5.2.9 Halaman Pembelian.....	86
5.2.10 Halaman Penambahan Saldo Kartu Pelanggan.....	87
BAB VI ANALISIS KINERJA PERANGKAT LUNAK.....	89
6.1 Pengujian Data Masukkan.....	89
BAB VII KESIMPULAN.....	97
7.1 Kesimpulan.....	97
7.2 Saran.....	98
Daftar Pustaka.....	99

DAFTAR TABEL

Tabel 1.1 Tabel <i>Contacts Smart Card</i>	16
Tabel 4.1 Tabel Spesifikasi Proses 1.1 Pengaturan Pelanggan.....	49
Tabel 4.2 Tabel Spesifikasi Proses 1.2 Personalisasi Kartu Pelanggan.....	50
Tabel 4.3 Tabel Spesifikasi Proses 2.1 Pengaturan Operator.....	52
Tabel 4.4 Tabel Spesifikasi Proses 2.2 Pengaturan Suplier.....	53
Tabel 4.5 Tabel Spesifikasi Proses 2.3 Pengaturan Barang.....	54
Tabel 4.6 Tabel Spesifikasi Proses 3. Pembelian.....	56
Tabel 4.7 Tabel Spesifikasi Proses 4. Penjualan.....	57
Tabel 4.8 Tabel Spesifikasi Proses 5. Isi Ulang Saldo Kartu.....	58
Tabel 4.9 Tabel Kamus Data.....	60
Tabel 4.10 Tabel Pengkodean Perusahaan.....	64
Tabel 4.11 Tabel Pengkodean Operator.....	64
Tabel 4.12 Tabel Pengkodean Pelanggan.....	65
Tabel 4.13 Tabel Pengkodean Administrator.....	65
Tabel 4.14 Tabel Keterangan Pengalamatan Memori pada Smart Card.....	67

DAFTAR GAMBAR

Gambar 1.1 <i>Smart Card</i> Tipe SLE4428.....	5
Gambar 1.2 <i>Smart Card Reader / Writer</i>	6
Gambar 2.1 Ukuran standar dan komponen <i>Smart Card</i>	15
Gambar 2.2 Karakteristik fisik sebuah <i>Smart Card</i>	15
Gambar 2.3 Delapan titik kontak dengan dunia luar.....	16
Gambar 2.4 Kontak elektrik <i>Smart Card</i>	21
Gambar 2.5 Notasi Proses	37
Gambar 2.6 Notasi Aliran Data	38
Gambar 2.7 Notasi Simpanan Data	38
Gambar 2.8 Notasi Terminator.....	38
Gambar 4.1 Struktur Pohon Proses Sistem Informasi Transaksi Prabayar	44
Gambar 4.2 Diagram Konteks Sistem Informasi Transaksi Prabayar	45
Gambar 4.3 DFD Level 1 Sistem Informasi Transaksi Prabayar.....	46
Gambar 4.4 DFD Level 2 dari proses 1. perosnalisasi pelanggan.....	47
Gambar 4.5 DFD Level 2 dari proses 2. pengaturan	48
Gambar 4.6 Rancangan antarmuka halaman login	68
Gambar 4.7 Rancangan antarmuka halaman konfigurasi jaringan.....	69
Gambar 4.8 Rancangan antarmuka halaman pengaturan operator	70
Gambar 4.9 Rancangan antarmuka halaman pengaturan barang	71
Gambar 4.10 Rancangan antarmuka halaman pengaturan supplier.....	72
Gambar 4.11 Rancangan antarmuka halaman pembelian.....	73
Gambar 4.12 Rancangan antarmuka halaman penjualan.....	74
Gambar 4.13 Rancangan antarmuka halaman personalisasi pelanggan.....	75
Gambar 4.14 Rancangan antarmuka halaman isi ulang saldo pelanggan.....	76
Gambar 5.1 Halaman Utama Sistem Informasi Transaksi Prabayar.....	79
Gambar 5.2 Halaman Konfigurasi Jaringan.....	80
Gambar 5.3 Halaman Login.....	81
Gambar 5.4 Halaman Pengaturan Operator.....	82
Gambar 5.5 Halaman Pengaturan Barang.....	83
Gambar 5.6 Halaman Pengaturan Supplier.....	84
Gambar 5.7 Halaman Personalisasi Pelangggan.....	85
Gambar 5.8 Halaman Penjualan.....	86

Gambar 5.9 Halaman Pembelian.....	87
Gambar 5.10 Halaman Isi Ulang.....	88
Gambar 6.1 Pengujian Pemasukkan Data Konfigurasi Jaringan.....	90
Gambar 6.2 Pengujian Pemasukkan Data Login Pemakai Sistem.....	90
Gambar 6.3 Pengujian Pemasukkan Data Operator yang tidak lengkap.....	91
Gambar 6.4 Pengujian Pemasukkan alamat email yang tidak benar.....	92
Gambar 6.5 Pengujian Pemasukkan Data Barang yang tidak lengkap.....	93
Gambar 6.6 Pengujian Pemasukkan Kode Barang yang tidak benar.....	93
Gambar 6.7 Pengujian Pemasukkan Data Suplier yang tidak lengkap.....	94
Gambar 6.8 Pengujian <i>Smart Card</i> yang tidak dapat dibaca.....	95
Gambar 6.9 Pengujian Pemasukkan PIN <i>smart card</i> yang salah.....	96



ABSTRAKSI

Salah satu strategi bisnis untuk meningkatkan volume penjualan adalah dengan sistem membayar dimuka atau sering diberi istilah prabayar. Dengan menggunakan strategi ini konsumen harus menyetujui aturan-aturan yang dibuat oleh penyedia jasa layanan prabayar agar dapat ikut menggunakan fasilitas yang diberikan. Kegiatan bisnis yang semakin berkembang akan ikut memacu perkembangan teknologi yang mendukung bisnis. Hal ini ditandai dengan munculnya berbagai alat elektronik pendukung aktifitas bisnis seperti *cash register*, *barcode reader*, *smart card* dan lainnya. Dengan menggunakan *smart card* dalam transaksi prabayar maka kedua pihak akan diuntungkan. Pihak penyedia jasa menjadi lebih mudah untuk meyakinkan calon konsumennya, sedangkan pihak konsumen akan merasa lebih aman karena *smart card* tersebut nantinya akan dipegang sendiri sehingga tidak mudah untuk dimanipulasi oleh pihak lain yang tidak berkepentingan.

Pada transaksi prabayar dibutuhkan tanda bukti bahwa konsumen mempunyai simpanan uang pada pihak penyedia jasa. Tanda bukti ini harus dapat diterima oleh kedua belah pihak dan bukti ini dapat dipegang pihak konsumen dimana pihak penyedia jasa tidak merasa keberatan dan tetap percaya bahwa data pada bukti tersebut sah dan aman. Sehingga permasalahan yang utama adalah data yang tercantum dalam bukti ini tidak dapat dimodifikasi secara sepihak. Jika pihak penyedia jasa akan

men-*debit* saldo maka diperlukan verifikasi dari pihak konsumen, demikian juga bila pihak konsumen akan menambah jumlah saldo maka harus ada verifikasi dari pihak penyedia jasa. Untuk menyimpan data agar aman digunakan media *smart card* serta mekanisme perlindungan data tambahan lain berupa enkripsi dan verifikasi.

Program simulasi transaksi prabayar yang dibuat ini menunjukkan bahwa media *smart card* sangat aman untuk menyimpan data karena telah memiliki mekanisme perlindungan data berupa PSC (*programmable Security Code*) dan *protection byte*. Didukung algoritma DES (*Data Encryption Standard*) untuk enkripsi dan algoritma anti duplikasi kartu maka media ini sangat cocok dijadikan sebagai bukti yang kuat untuk transaksi pembayaran

BAB I

PENDAHULUAN

1.1 Latar Belakang

Banyak sekali bentuk strategi bisnis yang dilakukan untuk meningkatkan volume penjualan. Salah satunya adalah dengan sistem membayar dimuka atau sering diberi istilah prabayar. Dengan menggunakan strategi ini konsumen harus menyetujui aturan-aturan yang dibuat oleh penyedia jasa layanan prabayar agar dapat ikut menggunakan fasilitas yang diberikan.

Sebelum teknologi berkembang seperti sekarang, pihak penyedia jasa harus dapat meyakinkan bahwa sistem yang mereka tawarkan sangat baik dan menguntungkan bagi konsumennya. Konsumen akan sangat dimudahkan dalam setiap kegiatan transaksi yang mereka lakukan. Ini sangat sulit karena landasan yang digunakan adalah kepercayaan terhadap penyedia jasa. Berbagai surat atau tanda bukti yang dipegang hanya dianggap sebagai referensi pembanding dan tidak bisa dijadikan jaminan yang kuat untuk mengajukan klaim jika terjadi sesuatu. Hal ini bisa terjadi karena data-data khususnya jumlah saldo yang dianggap valid dan dijadikan acuan dipegang oleh penyedia jasa. Penyedia jasa bisa berbuat apa saja dengan data tersebut, termasuk jika memang hendak berbuat suatu kecurangan misalnya dengan memanipulasi data jumlah

saldo dan membuat seolah-olah konsumen telah melakukan transaksi. Dari sini jelas terlihat bahwa posisi konsumen masih sangat lemah.

Kegiatan bisnis yang semakin berkembang akan ikut memacu perkembangan teknologi yang mendukung bisnis. Kita bisa melihat hal ini dengan munculnya berbagai alat elektronik pendukung aktifitas bisnis seperti *cash register*, *barcode reader*, *smart card* dan lain-lain. Tujuan utama dari alat-alat ini adalah selain sebagai alat untuk berhitung juga dipakai untuk menyimpan data-data transaksi. Data-data ini dapat diolah untuk menentukan strategi bisnis selanjutnya. Keanekaragaman media penyimpanan data dapat dilihat dari bentuk, kapasitas, juga fungsi tambahan lainnya. Contoh media penyimpanan adalah *hard disk*, *magnetic stripe*, *multimedia flash memory*, *smart card* dan lain-lain.

Smart card merupakan perangkat yang portable, sangat aman, harganya relative murah, dan mampu melakukan kalkulasi serta menyimpan data tentang pemakai *smart card* bersangkutan, maupun berbagai program dan sistem aplikasi sesuai keperluan dan kapasitas pada chip tunggal yang menyatu dalam kartu berlapis plastik tersebut. Keunggulan utama dalam sistem *smart card* terletak pada keamanan data berupa kode-kode rahasia yang tersimpan dalam kartu serta terintegrasinya sistem database yang akan memberikan pembatasan akses *smart card* secara kontinu.

Dengan menggunakan *smart card* dalam transaksi prabayar maka kedua pihak akan diuntungkan. Pihak penyedia jasa menjadi lebih mudah

untuk meyakinkan calon konsumennya, sedangkan pihak konsumen akan merasa lebih aman karena *smart card* tersebut nantinya akan dipegang sendiri sehingga tidak mudah untuk dimanipulasi oleh pihak lain yang tidak berkepentingan. Jika suatu waktu konsumen kehilangan *smart card*nya maka dia tidak perlu khawatir karena *smart card* itu sendiri sudah dilengkapi dengan mekanisme perlindungan data. Dengan demikian diharapkan kepercayaan konsumen terhadap penyedia jasa semakin meningkat juga tercipta suatu sistem yang adil dimana tidak ada lagi pihak yang diposisikan lebih lemah dan merasa dirugikan.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah bagaimana mengimplementasikan *smart card* untuk membangun Sistem Informasi Transaksi Prabayar pada sisi *client* yang aman dan adil bagi kedua belah pihak, baik konsumen maupun produsen di dalam tukar menukar informasi dan data transaksi.

Pada transaksi prabayar dibutuhkan tanda bukti bahwa konsumen mempunyai simpanan uang pada pihak penyedia jasa. Tanda bukti ini harus dapat diterima oleh kedua belah pihak sehingga bukti ini dapat dipegang salah satu pihak maka pihak yang lain tidak akan keberatan dan tetap percaya bahwa data pada bukti tersebut aman. Yang paling utama adalah data yang tercantum dalam bukti ini tidak dapat dimodifikasi secara sepihak. Jika pihak penyedia jasa akan men-*debit* saldo maka diperlukan

verifikasi dari pihak konsumen, demikian juga bila pihak konsumen akan menambah jumlah saldo maka harus ada verifikasi dari pihak penyedia jasa.

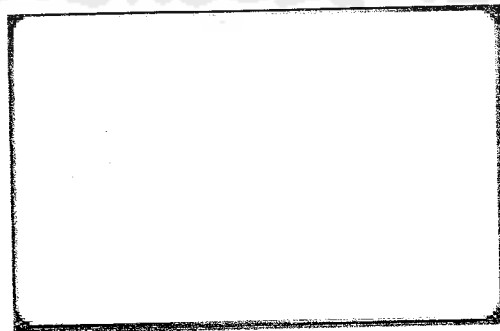
1.3 Batasan Masalah

Dalam penelitian ini penulis menggunakan batasan-batasan sebagai berikut :

- a. Sistem Informasi Transaksi Prabayar dengan media *smart card* pada sisi *client* ini dibangun untuk perusahaan bertipe usaha dagang secara retail yang semua *databasenya* terdapat pada server. Sistem ini dapat menangani :
 - Personalisasi pelanggan, yang meliputi pengaturan (*setup*) pelanggan dan personalisasi kartu (*smart card*) pelanggan.
 - Pengaturan (*setup*) operator, supplier (penyalur), dan barang.
 - Pengolahan data transaksi yang meliputi : transaksi penjualan barang kepada pelanggan secara prabayar menggunakan *smart card*, pembelian barang oleh perusahaan dari supplier, penambahan saldo atau isi ulang kartu (*smart card*) pelanggan.
- b. Sistem ini dirancang sebagai simulasi sistem prabayar yang menitikberatkan pada mengimplementasikan *smart card* pada sistem informasi transaksi prabayar. Sehingga di dalam sistem ini tidak dilengkapi pelaporan dan pencarian.

pada sistem informasi transaksi prabayar. Sehingga di dalam sistem ini tidak dilengkapi pelaporan dan pencarian.

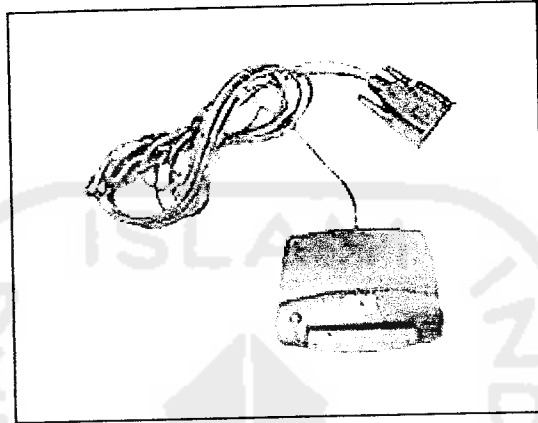
- c. Sistem informasi transaksi prabayar ini menggunakan algoritma DES (*Data Encryption Standard*), *random key generator* dan algoritma anti duplikasi *smart card* untuk keamanan data. Proses enkripsi dan dekripsi dengan algoritma DES akan menggunakan fungsi yang sudah disiapkan oleh pembuat *card reader* sebagai *software development kit* (SDK) dalam bentuk file DLL.
- d. Sistem yang di buat hanya menggunakan *hardware* tambahan sebagai berikut :
1. *Smart Card* dengan dengan jenis *memory*
Kartu ini tidak mempunyai *microprocessor*, tetapi mempunyai memori dan *control logic* yang mengatur akses unit baca tulis. *smart card* yang digunakan adalah tipe SLE-4428. tipe ini mempunyai 1024 x 8 bit EEPROM.



Gambar 1.1 *Smart Card* tipe SLE-4428

2. *Smart Card Reader / Writer*

Smart Card Reader / Writer adalah suatu antar muka untuk komunikasi antara kartu dengan computer.



Gambar 1.2 *Smart Card Reader / Writer*

3. Perangkat Jaringan

Jaringan dirancang hanya untuk menghubungkan *Client* dan *Server*, sesuai dengan kebutuhan sistem.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk membangun sebuah perangkat lunak yang dapat menangani transaksi secara prabayar yang menitikberatkan pada pengimplementasian *smart card* sebagai media komunikasi dan keamanan data.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah menciptakan sistem pelayanan terhadap publik yang memberikan kemudahan dalam tukar-menukar informasi, transaksi, dengan tingkat keamanan yang tinggi.

1.6 Metodologi Penelitian

1.6.1 Metode Pengumpulan Data

1.6.1.1 Data Primer

Teknik pengumpulan data yang dilakukan dalam penyusunan tugas akhir ini adalah sebagai berikut :

a. Metode Observasi

Metode Pengamatan (Observasi), pengumpulan data yang dilakukan dengan mengadakan pengamatan secara langsung di lapangan.

b. Metode Wawancara

Metode wawancara atau tanya jawab langsung dengan pihak-pihak yang terkait untuk memperoleh data yang tepat sehingga perancangan aplikasi tidak menyimpang dari tujuan semula.

c. Metode *Library Research*

Metode kepustakaan (*Library Research*), mengumpulkan data yang dilakukan dengan mengumpulkan data dari buku-buku referensi, jurnal-jurnal yang didapat di internet, dan

literatur-literatur tugas akhir yang relevan dengan permasalahan.

1.6.1.2 Data Sekunder

Data sekunder sebagai penunjang penyusunan tugas akhir ini didapat dengan cara pengumpulan data dengan metode :

- a. Literatur
Mempelajari ketersediaan data yang telah diperoleh di lapangan.
- b. Telaah Dokumen
Mempelajari dokumen artikel dan catatan lain yang berkaitan dengan permasalahan.

1.6.2 Metode Pengembangan Sistem

1.6.2.1 Analisa Kebutuhan

Sejalan dengan perkembangan teknologi maka kebutuhan akan aplikasi yang dapat memudahkan berbagai operasional kerja dengan otomatisasi, efektifitas, *privacy*, dan keamanan yang tinggi sangatlah diinginkan.

1.6.2.2 Perancangan Sistem

Pembuatan sistem terdiri dari beberapa tahap perancangan, yaitu:

- a. Pembuatan diagram alir data atau *Data Flow Diagram* (DFD), yang menjelaskan mulai dari *Context Diagram* sampai dengan DFD turunan sebagai penjelasan dari

Context Diagram yang dibuat, spesifikasi proses, kamus data, dan aturan pengkodean.

- b. Perancangan area memori pada *smart card* (*memory mapping*), yang digunakan untuk menentukan pengalokasian data pada *smart card*.
- c. Perancangan antarmuka, yang digunakan untuk memberikan gambaran tentang perangkat lunak yang telah dibuat.

1.6.2.3 Implementasi Sistem

Setelah perancangan sistem dilakukan, maka hasil perancangan tersebut dapat diimplementasikan.

1.6.2.4 Analisis Kinerja Perangkat Lunak

Analisis kinerja perangkat lunak diperoleh dari implementasi sistem yang disempurnakan.

1.7 Sistematika Penulisan

Untuk memberikan gambaran secara menyeluruh masalah yang akan dibahas dalam laporan ini, maka sistematika laporan dibagi dalam tujuh bab, sebagai berikut :

Bab I Pendahuluan

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan laporan tugas akhir.

Bab II Landasan Teori

Bagian ini memuat teori-teori tentang Sistem, Informasi, Sistem Informasi, *Smart Card*, *Smart Card Reader*, Sistem Informasi Berbasis *SmartCard*, Kriptografi, DES (*Data Encryption Standard*), Teknik Perancangan Sistem.

Bab III Analisis Kebutuhan Perangkat Lunak

Bab ini memuat tentang metode analisis dan hasil analisis perangkat lunak Sistem Informasi Transaksi Prabayar berbasis *Smart Card*.

Bab IV Perancangan Perangkat Lunak

Bab ini memuat tentang metode perancangan dan hasil perancangan perangkat lunak Sistem Informasi Berbasis *SmartCard*.

Bab V Implementasi Perangkat Lunak

Bab ini memuat implementasi dari perangkat lunak yang dihasilkan.

Bab VI Analisis Kinerja Perangkat Lunak

Bab ini berisi dokumentasi hasil pengujian terhadap perangkat lunak yang dihasilkan, berkaitan dengan kesesuaian hasil perangkat lunak dengan kebutuhan perangkat lunak tersebut seperti yang telah diuraikan pada bab sebelumnya.

Bab VII Kesimpulan

Dalam bab ini akan disimpulkan hasil dari pengujian dan pembahasan serta saran yang perlu diperhatikan berdasar keterbatasan-

keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan tugas akhir.



BAB II

LANDASAN TEORI

2.1 Sistem

Sistem merupakan cara pandang terhadap dunia nyata yang terdiri dari elemen-elemen yang saling berinteraksi untuk mencapai tujuan dalam lingkungan yang kompleks [SIM95]. Sistem juga didefinisikan sebagai suatu kumpulan objek yang terangkai dalam interaksi dan saling ketergantungan yang teratur. Definisi lain dari sistem adalah sebagai kumpulan elemen yang saling berinteraksi membentuk kesatuan, dalam interaksi yang kuat maupun lemah dengan pembatas yang jelas [SUR98].

2.2 Informasi

Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi penerimanya [JOG99]. Menurut pustaka lain, Informasi juga memiliki pengertian data yang telah diproses, atau data yang memiliki arti [McL98].

Sumber dari Informasi adalah data. Data terdiri dari fakta – fakta dan angka – angka yang relatif tidak berarti bagi pemakai [McL98]. Data adalah unit Informasi dalam format tertentu. Semua software dibagi ke dalam dua kategori : data dan program. Program adalah sekumpulan instruksi untuk

memanipulasi data. Data dapat berupa angka, teks pada kertas, *bit* atau *byte* yang tersimpan pada memori elektronik, atau fakta yang ada dalam pikiran manusia [WAH02].

Teori lain menyatakan Informasi terdiri dari data-data yang telah diambil kembali, diolah, atau sebaliknya dipergunakan untuk tujuan informatif atau kesimpulan, argumentasi atau sebagai dasar untuk peramalan pengambilan keputusan [SUR98].

2.3 Sistem Informasi

Sistem Informasi adalah suatu Sistem manusia-mesin yang terpadu untuk menyajikan Informasi guna mendukung fungsi operasi, manajemen, dan pengambilan keputusan dalam organisasi.

Tujuan Sistem Informasi adalah untuk menyediakan dan menSistematikakan Informasi yang merefleksikan seluruh kejadian atau kegiatan yang diperlukan untuk mengendalikan operasi-operasi organisasi. Sedangkan kegiatannya adalah mengambil, mengolah, menyimpan, dan menyampaikan Informasi yang diperlukan untuk terjadinya komunikasi yang diperlukan untuk mengoperasikan seluruh aktifitas di dalam organisasi. [BUD95].

2.4 **Smart card**

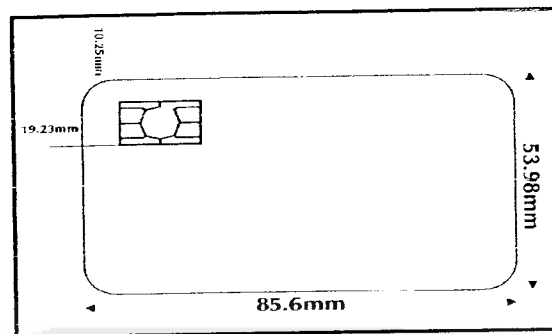
Smart card adalah kartu plastik yang berukuran sama dengan kartu kredit yang di dalamnya terdapat *chip* silikon yang disebut *microcontroller*. *Chip* merupakan *integrated circuit* yang terdiri dari prosesor dan memori. *Chip*, seperti layaknya CPU (*Central Processing Unit*) di komputer, bertugas melaksanakan perintah dan menyediakan *power* ke *Smart card*. *Smart card* mempunyai kemampuan untuk memproses dan menginterpretasikan data, serta menyimpan data tersebut secara aman [EVE99].

2.4.1 **Standarisasi Smart card**

Smart card telah di standarisasi baik kapasitas fisiknya maupun *command interface*-nya. Standar dari *command interface* telah ditetapkan sedemikian rupa. Penamaan perintah-perintah dari suatu *command* sudah ditetapkan, sehingga para pengembang dapat dengan mudah membuat aplikasinya. Begitu juga dengan interoperabilitas antara Sistem yang berbeda. Standarisasi ini membuat perbedaan di antara produk-produk *Smart card* yang ada, bukanlah penghalang dalam mengembangkan suatu aplikasi.

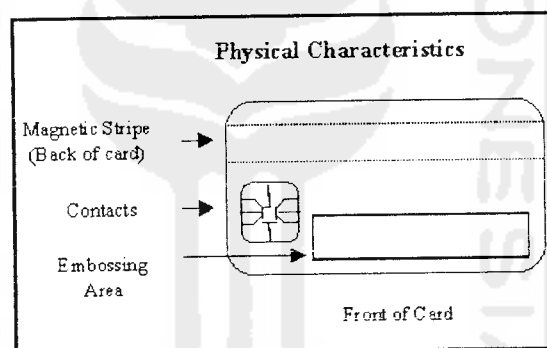
Ukuran standar dan komponen *Smart card* menurut ISO 7816 adalah [EVE99] :

1. Dimensi Kartu, yaitu panjang 87,6 mm, lebar 53,98 mm dan tebal 0,76 mm
2. Kartu tersebut terbuat dari PVC (*Polyvinyl Chloride*) atau PVCA (*Polyvinyl Chloride Acetate*)



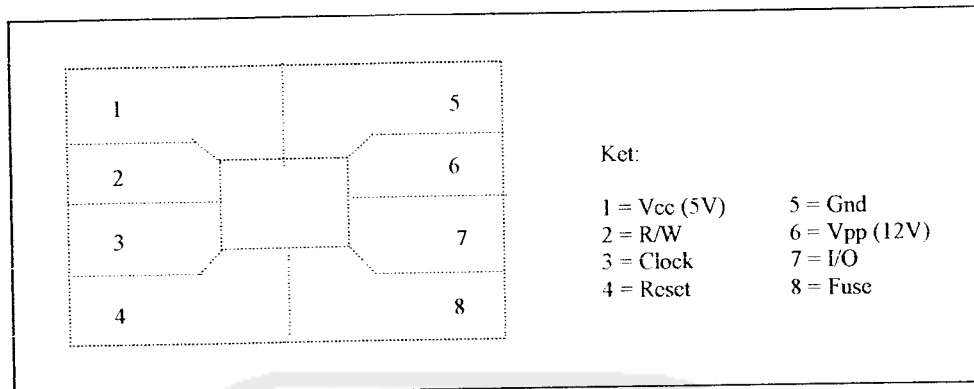
Gambar 2.1 Ukuran standar dan komponen *Smart card*

Karakter fisik dari *Smart card* berdasar standar ISO 7816 dapat anda lihat pada beberapa aplikasi seperti Kartu kredit, kartu ATM dan sebagainya seperti Gambar 2.2



Gambar 2.2 Karakteristik fisik sebuah *Smart card*

Normalnya, sebuah *Smart card* tidak memiliki catu daya, layar, atau keyboard. *Smart card* berinteraksi dengan dunia luar menggunakan antarmuka komunikasi serial lewat delapan titik kontak atau *contact point* yang ada.



Gambar 2.3 Delapan titik kontak dengan dunia luar

ISO (*International Standard Organization*) 7816 [GUT99] :

- ISO 7816-1 : Atribut fisik
Memberikan standarisasi tentang karakteristik fisik dari *Integrated Circuit Card (IC Card)*
- ISO 7816-2 : Menyatakan dimensi dan lokasi dari *Contacts*

Tabel 1. *Contacts Smart Card*

Contact	Designation	Kegunaan
C1	Vcc (Sumber Tegangan)	Tempat penerimaan aliran listrik yang diberikan oleh <i>reader</i>
C2	RST (Sinyal Reset)	<i>Reset line</i> . Melalui jalur ini, IFD bisa memberi <i>signal</i> kepada <i>chip microprocessor Smart card</i> untuk melakukan <i>reset sequence of instructions</i>
C3	CLK (Sinyal Clock)	<i>Clock signal line</i> , merupakan jalur untuk memasukkan <i>clock signal</i> kedalam <i>microprocessor chip</i>
C4	RFU (Reserved for Future Use)	Digunakan untuk beberapa tahun kedepan
C5	GND (Ground)	<i>Ground line</i> , menyediakan <i>electrical ground</i> antara IFD dan ICC
C6	Vpp (Tegangan Pemrograman)	Pemrograman koneksi listrik digunakan untuk memprogram EEPROM dari generasi pertama ICCs
C7	I/O (Input / Output Data)	Masukkan dan keluaran yang menghasilkan komunikasi <i>half-duplex channel</i> antara <i>reader</i> dan <i>Smart card</i>
C8	RFU (Reserved for Future Use)	Digunakan untuk beberapa tahun kedepan

- ISO 7816-3 : Sinyal dan protokol

Bagian ini menjelaskan tentang sinyal elektronik dan protokol tranmisi dari *Integrated Circuit Card*

- ISO 7816-4 : *Inter-industry commands for interchange*

- Isi dari suatu pesan, perintah dan respon, dikirimkan melalui suatu antar muka menuju kartu begitupun sebaliknya.
- Struktur dan isi dari *byte* yang telah dikirim kartu selama *answer to reset*.
- Struktur dan metode akses file.
- Metode akses untuk algoritma yang digunakan oleh kartu.

- ISO 7816-5 : *Numbering system and registration procedure for application indentifiers*.

Menetapkan standarisasi untuk *application indentifiers* (AIDs). AIDs mempunyai dua bagian. Yang pertama adalah *Registered Application Provider Indentifiers* (RIDs) yang terdiri dari 5 *byte*, masing-masing vendor memiliki RID yang unik. Bagian kedua adalah panjang variabel yang terdiri dari 11 *byte* yang digunakan RIDs untuk *indentifier* aplikasi yang spesifik.

- ISO 7816-6 : *Inter-industry data elements*

Menggambarkan aturan data yang dibutuhkan dalam beberapa aplikasi.

- ISO 7816-7 : *Inter-industry commands for Structured Card Language (SCQL)*

Menetapkan beberapa perintah untuk mengakses isi dari *Smart card* dan struktur relasi *database*.

2.4.2 Jenis *Smart card*

Berdasarkan teknologinya, *Smart card* dapat dibedakan menjadi 3 jenis, yaitu [EVE99] :

- *Memory Card*

Ini adalah jenis pertama yang dikenal orang dan digunakan pertama kali untuk kartu telepon. Jenis kartu ini menyimpan data yang telah di *preload* oleh manufakturnya, kemudian mesin pembaca akan mengurangi isi variabel yang disimpannya.

- *Microprocessor Card*

Kartu jenis ini dapat diprogram dengan bebas untuk keperluan apa saja. Hal ini dimungkinkan dengan adanya mikroprosesor dalam *chip*. Keterbatasannya ada pada ukuran ROM yang dimiliki dan fungsi aritmatika yang masih sederhana

- *Contactless Card*

Kartu jenis ini mentranfer data tanpa ada kontak elektrik antara kartu dan terminalnya. Dapat berupa *memory card* atau *microprocessor card*

1. **Memory Card**

Memory Card tidak mempunyai kemampuan khusus untuk memproses data dan tidak dapat mengatur data secara dinamis. Untuk berkomunikasi dengan *reader* digunakan *synchronous* protokol. Ada 3 tipe *memory cards* [EVE99] :

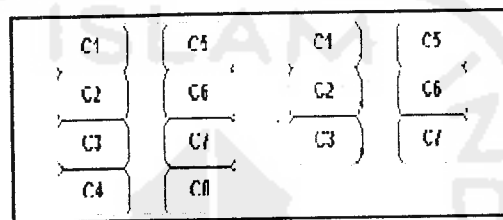
- *Straight Memory Cards*

Kartu tipe ini hanya menyimpan data dan tidak mempunyai kemampuan memproses data sehingga lebih mirip dengan disket biasa namun mempunyai kemampuan mekanisme untuk penguncian. Kartu ini juga tidak dapat mengidentifikasi secara langsung ke *reader*, sehingga program mencari tahu tipe kartu apa yang sedang ada dalam *reader*.

- *Protected / Segmented Memory Cards*

Kartu ini memiliki kontrol logika untuk mengakses memori dari kartu. Kontrol Logika ini biasanya disebut *Intellegent Memory Cards* karena dapat diset untuk memproduksi beberapa atau seluruh *array* memori. Kartu ini dapat pula diset hanya untuk dibaca atau ditulis atau kedua-duanya. Cara ini dilakukan menggunakan *password* atau kunci Sistem. Kartu ini dapat dibagi secara *logical* dalam beberapa bagian untuk bermacam-macam fungsi.

atau terminal (*Card Reader*) hanya satu pihak yang dapat berkomunikasi dalam satu waktu. Komunikasi ini biasa disebut dengan komunikasi *half duplex*. Komunikasi selalu diinisialisasi atau dimulai oleh terminal dimana hubungan relasi antara kartu dengan terminal hampir sama dengan *client-server* [EVE99].



Gambar 2.4 Kontak elektrik *Smart card*

2.5 *Smart card Reader / Writer*

Smart card Reader / Writer adalah suatu antar muka untuk komunikasi antara kartu dengan komputer. Setiap tipe dari *Smart card* mempunyai perintah dan protocol komunikasi yang berbeda. Antar muka antara *Smart card* dan *Smart card reader* mengikuti spesifikasi dari ISO 7816-3 dengan beberapa batasan atau penyempurnaan untuk meningkatkan fungsionalitas dari *Smart card reader / writer*. Antar muka dari suatu *Smart card* terdiri dari *Smart card power supply*, pemilihan kartu, dan antar muka *microcontroller*.

2.6 Aplikasi berbasis *Smart card*

Sistem aplikasi yang berbasis *Smart card* merupakan kumpulan komponen yang saling bekerja sama dalam membentuk layanan aplikasi bagi

pengguna akhir dengan melibatkan *Smart card* sebagai bagian dari Sistem. Umumnya, *Smart card* digunakan sebagai media penyimpan data terbatas seperti nomor identitas, *password*, digital signature, nomor rekening, dan sebagainya.

Aplikasi penggunaan *Smart card* dapat digolongkan menjadi 3 kategori:

1. Penyimpanan Data

Kartu digunakan sebagai alat penyimpan Informasi yang menyenangkan, *portable*, dan aman (misal, rekam medis)

2. Identifikasi

Kartu menjadi alat yang aman untuk mengidentifikasi sipemegang kartu dan memberi akses tertentu kepada pemegang kartu (misal, otorisasi akses *Personal Computer*)

3. Keuangan

Kartu digunakan untuk transaksi sebagai pengganti uang (misal, Kartu Debit)

2.7 Kriptografi

Kriptografi adalah proses menjaga keamanan informasi yang dikirim melalui jaringan publik, seperti internet , dengan enkripsi yang membuat informasi tidak dapat dibaca oleh orang yang tidak mempunyai *key* untuk

mendekripsikannya [WAH02]. Kriptografi adalah ilmu yang mempelajari tentang suatu teknik matematika yang berhubungan dengan aspek keamanan data atau informasi seperti *confidentiality*, *data integrity*, *entity authentication*, dan *data origin authentication* [VAN96]. Fungsi-fungsi yang mendasar dalam kriptologi adalah enkripsi dan dekripsi.

Enkripsi (*encryption*) adalah proses mengubah data kedalam bentuk yang hanya dapat dibaca oleh penerima (*receiver*) yang diinginkan. Untuk membaca data yang terenkripsi penerima harus menggunakan kunci dekripsi (*decryption key*). Pada skema enkripsi tradisional, pengirim (*sender*) dan penerima menggunakan kunci yang sama untuk mengenkripsikan dan mendekripsikan data. Pada skema enkripsi kunci publik (*public-key encryption*) digunakan dua kunci : kunci publik (*public-key*) yang dapat digunakan oleh semua orang dan kunci *privat* (*private key*) yang hanya dimiliki oleh orang yang membuatnya. Dengan metode ini, semua orang dapat mengirimkan data yang terenkripsi tetapi hanya pemilik kunci *privat* yang dapat mendekripsikannya [WAH02].

2.7.1 Kunci Simetris

Ini adalah jenis kriptografi yang paling umum digunakan. Kunci untuk membuat pesan (*plaintext*) yang disandikan sama dengan kunci untuk membuka pesan yang disandikan ini. Jadi pembuat pesan dan penerima pesan harus mempunyai kunci yang sama persis. Siapapun yang memiliki

kunci tersebut termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia pesan (*chipertext*).

2.7.2 DES (*Data Encryption Standard*)

Standar ini dibuat oleh National Bureau of Standard USA pada tahun 1977. DES merupakan *block cipher* yang beroperasi dengan blok berukuran 64-bit dan kunci 56-bit. *Brute-force attack* terhadap DES membutuhkan kombinasi 2 pangkat 56, atau sekitar 7×10 pangkat 16, atau 70 juta milyar, algoritma enkripsi ini termasuk yang kuat dan tidak mudah diterobos. Cara enkripsi ini telah dijadikan standar oleh pemerintah Amerika Serikat sejak tahun 1977 dan menjadi standar ANSI tahun 1981.

DES seharusnya terdiri dari algoritma enkripsi data yang diimplementasikan dalam peralatan elektronik untuk tujuan tertentu. Peralatan ini dirancang menurut cara yang mereka gunakan dalam sistem atau jaringan komputer untuk melengkapi perlindungan *cryptographic* pada data biner.

Metode implementasi akan tergantung pada aplikasi dan lingkungan disekitar sistem itu. Peralatan itu diimplementasikan tetapi sebelumnya diuji dan divalidkan secara akurat untuk menampilkan transformasi dalam bentuk algoritma.

DES bekerja berdasarkan bit yang biasa dikenal dengan 0 dan 1 (basis 2) atau disebut juga bilangan biner. Setiap kelompok 4 bit akan membentuk satu bilangan heksa desimal (basis 16). Bilangan biner "0001"

sama dengan "1" pada heksa desimal, "1000" biner = "8" heksa, "1001" biner = "9" heksa, sedangkan "1010" biner = "A" heksa dan "1111" biner = "F" heksa.

Dalam prosesnya DES adalah mengenkripsi 64 bit pesan yang terbagi secara berkelompok, yang ternyata sama dengan 16 heksa. Untuk melakukan enkripsi, DES menggunakan kunci yang panjangnya mendekati 16 heksa atau 64 bit. Kenyataannya pada algoritma ini setiap bit ke-8 akan diabaikan sehingga yang efektif hanya 56 bit [KRI03].

2.7.3 Algoritma DES

1. Proses Kunci

- 1.1 Ambil kunci sepanjang 64 bit. (Setiap bit ke-8 dianggap sebagai bit pariti. Untuk mendapatkan pariti yang benar pada sebuah kunci, setiap byte harus berisi angka ganjil "1" bit).
- 1.2 Hitung *key schedule*.
 - 1.2.1 Lakukan permutasi pada kunci 64 bit. (Bit pariti diabaikan, sehingga mengurangi kunci menjadi 56 bit. Setelah dilakukan permutasi bit pertama akan menjadi bit ke-57, bit 2 akan menjadi bit ke-49 dan seterusnya hingga bit ke-56 menjadi bit ke-4).

Permuted Choice 1 (PC-1)

57 49 41 33 25 17 9

1 58 50 42 34 26 18

10 2 59 51 43 35 27

19 11 3 60 52 44 36

63 55 47 39 31 23 15

7 62 54 46 38 30 22

14 6 61 53 45 37 29

21 13 5 28 20 12 4

1.2.2 Pisahkan kunci yang telah dipermutasi menjadi 2 bagian. 28 bit yang pertama disebut C[0] and 28 bit berikutnya disebut D[0].

1.2.3 Hitung 16 *subkeys*. Dimulai $i = 1$.

1.2.3.1 Lakukan 1 atau 2 pergeseran secara berulang ke kiri pada kedua C[i-1] dan D[i-1] untuk mendapatkan C[i] dan D[i] secara terus menerus. Jumlah pergeseran setiap iterasi akan ditunjukkan pada tabel dibawah.

Iterasi #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Geser Kiri	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

1.2.3.2 Permutasikan secara berurutan $C[i]D[i]$ seperti ditunjukkan di bawah. Proses ini akan menghasilkan $K[i]$ yang panjangnya sebesar 48 bit.

Permuted Choice 2 (PC-2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
44	49	39	56	34	53
46	42	50	36	29	32

1.2.3.3 Kembali ke 1.2.3.1 sampai $K[16]$ selesai dihitung

2. Proses 64 bit blok data.

2.1 Dapatkan data blok 64 bit. Jika blok kurang dari 64 bit, maka harus ditambahkan agar sesuai apa yang dibutuhkan aplikasi.

2.2 Lakukan permutasi berikut pada blok data.

Initial Permutation (IP)

58 50 42 34 26 18 10 2

60 52 44 36 28 20 12 4

62 54 46 38 30 22 14 6

64 56 48 40 32 24 16 8

57 49 41 33 25 17 9 1

59 51 43 35 27 19 11 3

61 53 45 37 29 21 13 5

63 55 47 39 31 23 15 7

2.3 Pisahkan setiap blok data menjadi 2 bagian. 32 bit yang pertama disebut L[0] dan 32 bit berikutnya adalah R[0].

2.4 Masukkan 16 *subkeys* pada data blok. Dimulai dari $i = 1$.

2.4.1 Ubah 32 bit $R[i-1]$ menjadi 48 bit berdasarkan fungsi pemilihan bit.

Expansion (E)

32 1 2 3 4 5

4 5 6 7 8 9

8 9 10 11 12 13

12 13 14 15 16 17

16 17 18 19 20 21

20 21 22 23 24 25

24 25 26 27 28 29

28 29 30 31 32 1

2.4.2 *Exclusive-or* (xor) $E(R[i-1])$ dengan $K[i]$.

2.4.3 Pecahkan $E((R[i-1]) \text{ xor } K[i])$ menjadi 6 buah 6 bit blok. Bit 1-6 adalah $B[1]$, bit 7-12 adalah $B[2]$, dan seterusnya sampai bit 43-48 menjadi $B[8]$.

2.4.4 Substitusi nilai yang didapatkan pada *S-boxes* untuk setiap $B[j]$. Dimulai dari $i = 1$. Semua nilai yang tersimpan pada *S-boxes* harus terdiri atas 4 bit.

2.4.4.1 Ambil bit pertama dan ke-6 $B[j]$ secara bersama-sama sebagai nilai 2 bit (misalkan sebagai m) mengindikasikan baris pada $S[j]$ yang dicari untuk proses substitusi.

2.4.4.2 Ambil bit ke-2 sampai 5 dari $B[j]$ lalu digabung sebagai nilai 4 bit (misalkan sebagai n) mengindikasikan sebagai kolom pada $S[j]$ untuk mencari substitusi.

2.4.4.3 Tukarkan $B[j]$ dengan $S[j][m][n]$.

Substitution Box 1 (S[1])

14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
 0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8
 4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0
 15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13

S[2]

15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10
 3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5
 0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15
 13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9

S[3]

10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8
 13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1
 13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7
 1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12

S[4]

7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15
 13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9
 10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4
 3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14

S[5]

2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9
 14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6

4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14
 11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3

S[6]

12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11
 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8
 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6
 4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13

S[7]

4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1
 13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6
 1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2
 6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12

S[8]

13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7
 1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2
 7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8
 2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11

2.4.4.4 Kembali ke 2.4.4.1 sampai seluruh 8 blok tertukar.

2.4.5 Permutasi secara berurutan B[1] sampai B[8] seperti terlihat di bawah.

Permutation P

16 7 20 21

29 12 28 17

1 15 23 26

- *Strored Value Memory Cards*

Kartu ini didesain khusus secara spesifik untuk menyimpan nilai atau *point*. Kebanyakan digunakan untuk keperluan keamanan perusahaan dalam hal menghitung nilai atau *point*. Array pada memori dirancang untuk terus berkurang jika digunakan. Jika unit memori sudah habis maka kartu tidak dapat digunakan lagi. Untuk dapat menggunakannya lagi kartu harus diisi ulang. Contohnya pada kartu telepon *chip*.

2.4.3 Jenis Memori Pada *Smartcard*

Secara umum menurut ISO7816-95 ada 3 jenis memori yang digunakan:

- ROM (*Read Only Memory*), berfungsi untuk menyimpan program utama dan sifatnya permanen.
- RAM (*Random Access Memory*), berfungsi untuk menyimpan data sementara ketika proses sedang berjalan atau hasil penghitungan selama mengeksekusi perintah.
- EEPROM (*Electrically Erasable Programmable Read Only Memory*), berfungsi untuk menyimpan program dan data yang sewaktu-waktu bisa diubah.

2.4.4 Komunikasi pada *Smart card*

Semua komunikasi dari *Smart card* menggunakan C7 *contact*, seperti kita lihat pada gambar 2.4. Dalam melakukan komunikasi, baik pihak kartu

5 18 31 10
 2 8 24 14
 32 27 3 9
 19 13 30 6
 22 11 4 25

2.4.5.1 *Exclusive-or* (xor) hasilnya dengan $L[i-1]$. Jadi secara

keseluruhan, $R[i] = L[i-1] \text{ xor}$

$P(S[1](B[1])...S[8](B[8]))$, dimana $B[i]$ adalah blok data 6 bit dari $E(R[i-1]) \text{ xor } K[i]$. (Fungsi untuk $R[i]$ ditulis sebagai

$R[i] = L[i-1] \text{ xor } f(R[i-1], K[i])$).

2.4.6 $L[i] = R[i-1]$.

2.4.7 Kembali ke 2.4.1 sampai $K[16]$ dikerjakan.

2.5 Lakukan permutasi berikut pada blok $R[16]L[16]$

Final Permutation (IP^{*-1})

40 8 48 16 56 24 64 32
 39 7 47 15 55 23 63 31
 38 6 46 14 54 22 62 30
 37 5 45 13 53 21 61 29
 36 4 44 12 52 20 60 28
 35 3 43 11 51 19 59 27
 34 2 42 10 50 18 58 26

33 1 41 9 49 17 57 25

Untuk melakukan dekripsi gunakan langkah yang sama, namun gunakan kunci $K[i]$ secara terbalik.

2.8 *Programmable Security Code (PSC)*

Merupakan kode yang digunakan untuk proses verifikasi ketika akan menulis data pada kartu. Pada tipe kartu SLE 4428, mempunyai ukuran sebesar 2 byte. Pada umumnya, kartu yang baru dikeluarkan oleh pabrik, mempunyai PSC *default* "FFFF". Demi alasan keamanan pada saat personalisasi nilai dari PSC akan diubah sesuai dengan aturan atau algoritma dari aplikasi program.

Pada SLE 4428, PSC terletak pada alamat 1022-1023. Isi dari alamat ini tidak dapat dibaca oleh program, untuk mengetahui isi dari alamat PSC, maka dilakukan dengan cara verifikasi. Kemudian apabila verifikasi berhasil, *error counter smart card* dengan alamat 1021 tidak terjadi perubahan, yaitu bernilai "FF" (1111 1111). Apabila terjadi kesalahan di dalam verifikasi, maka *error counter* akan berubah digit menjadi 1 menjadi 0 dimana (1111 1111) → (1111 1110), demikian seterusnya sampai menjadi (0000 0000) dan kartu akan hangus atau *fuse* terputus.

2.9 *Random Key Generator*

Untuk melakukan pengacakan PSC setelah dilakukan personalisasi, maka saat penggantian PSC yang baru akan dilakukan pengacakan PSC yang mempunyai batas 0x0 sampai dengan 0xF. Parameter yang digunakan untuk pengacakan tidak dipublikasikan dalam dokumentasi teknik, dengan alasan keamanan data.

2.10 *Protection Byte*

Untuk melakukan perlindungan data pada alamat tertentu yang disimpan pada *smart card* maka SLE 4428 juga dilengkapi dengan fasilitas *protection byte*, yaitu *flag* yang dapat diubah menjadi aktif. Ketika *flag* diatur menjadi aktif maka data yang ditandai hanya dapat dibaca dan tidak dapat ditulis kembali. Alamat yang sudah diaktifkan sebagai *protection byte* tidak dapat diubah kembali dan bersifat tetap, artinya data pada alamat tersebut akan menjadi tetap pula.

Protection byte dapat dilakukan pada semua alamat pada *smart card* kecuali alamat tempat PSC tersimpan.

2.11 Algoritma Anti Duplikasi Kartu

Pada penelitian ini, dibuat algoritma untuk mendeteksi keaslian kartu yang telah dipersonalisasi oleh program aplikasi. Alasan utama diciptakan algoritma anti duplikasi kartu adalah sangat mudah untuk membaca dan menuliskan isi kartu pada *smart card* yang lain. Sebagai contoh *smart card A* dengan data tertentu dan PSC "FFAA", kemudian dituliskan pada *smart card* baru yang mempunyai default PSC "FFFF", maka tanpa algoritma anti duplikasi kartu, program aplikasi akan mengakses data dengan data-data yang sama dituliskan dari *smart card A*.

Dengan adanya algoritma anti duplikasi kartu, maka program dapat mengecek keaslian *smart card*. Langkah-langkah pada algoritma ini terbagi menjadi dua bagian yaitu personalisasi dan pembacaan *smart card*.

Proses personalisasi

Langkah-langkah yang dilakukan pada saat personalisasi kartu adalah :

1. Memeriksa apakah alamat pada *smart card* yang akan digunakan untuk menyimpan data masih kosong dan tidak terproteksi
2. Verifikasi PSC apakah masih "FFFF", jika kedua langkah ini benar maka kartu dianggap masih kosong.
3. Menuliskan data pada *smart card* sesuai dengan spesifikasi rancangan pengalaman.

4. Mengacak PSC, dan ditemukan PSC yang baru.
5. Mengenkripsi PSC yang baru dengan kunci rahasia menggunakan algoritma DES dan menuliskan hasil enkripsi pada alamat yang sudah ditentukan.
6. Mengganti PSC yang lama "FFFF" dengan PSC yang baru.

Proses pembacaan kartu

Langkah-langkah yang dilakukan pada saat pembacaan kartu adalah :

1. Setelah kartu terdeteksi program aplikasi, maka dilakukan pengecekan apakah data pada *smart card* sesuai dengan rancangan pengalamatan dan proteksi memori.
2. Mengecek PSC, dengan cara mendekripsi data pada alamat hasil enkripsi dari PSC dengan kunci rahasia menggunakan algoritma DES.
3. Melakukan verifikasi PSC dan membaca *error counter* apakah nilainya berkurang.
4. Jika nilai berkurang, maka dipastikan kartu palsu.

2.12 Teknik Perancangan Sistem

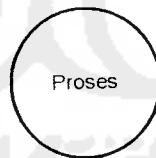
2.12.1 Diagram Konteks (*Context Diagram*)

Context Diagram (CD) adalah kasus khusus dari *Data Flow Diagram* (DFD) yaitu bagian dari DFD yang berfungsi memetakan model lingkaran yang direpresentasikan dengan lingkaran tunggal yang mewakili keseluruhan sistem [HUS97].

Komponen-komponen Data Flow Diagram adalah :

1. Proses

Proses menunjukkan transformasi dari masukan menjadi keluaran, dalam hal ini sejumlah masukan dapat menjadi hanya satu keluaran ataupun sebaliknya. Proses direpresentasikan dalam bentuk lingkaran, oval, atau bujursangkar. Salah satu contoh notasi proses yang berbentuk oval dapat dilihat pada gambar 2.5.

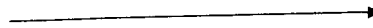


Gambar 2.5 Notasi Proses

2. Alir Data

Komponen ini direpresentasikan dengan menggunakan panah yang menuju ke atau dari proses. Digunakan untuk menggambarkan gerakan paket data dari suatu bagian ke bagian lain dari sistem

dimana penyimpanan mewakili lokasi penyimpanan data. Notasi alir data dapat dilihat pada gambar 2.6.



Gambar 2.6 Notasi Aliran Data

3. **Penyimpanan Data**

Komponen ini digunakan untuk memodelkan kumpulan data atau paket data. Notasi yang digunakan adalah garis sejajar, segi empat dengan sudut melengkung atau persegi panjang. Salah satu contoh notasi simpanan data dapat dilihat pada gambar 2.7.



Gambar 2.7 Notasi Simpanan Data.

4. **Terminator**

Komponen berikutnya adalah terminator yang direpsentasikan menggunakan persegi panjang, yang mewakili entiti luar dimana sistem berkomunikasi. Contoh dari notasi terminator atau entiti luar sistem dapat dilihat pada gambar 2.8.



Gambar 2.8 Notasi Terminator.

BAB III

ANALISIS KEBUTUHAN PERANGKAT LUNAK

3.1 Metode Analisis

Metode analisis yang digunakan dalam pengembangan sistem ini adalah metode deskriptif analisis yaitu suatu metode yang memusatkan pemecahan masalah pada masa sekarang. *Descriptive Research* adalah penelitian yang dilakukan dengan cara membuat deskripsi permasalahan yang telah diidentifikasi.

Untuk melakukan suatu pengembangan sistem dibutuhkan suatu metodologi pengembangan sistem. Metodologi pengembangan sistem adalah kesatuan metode-metode, konsep-konsep pekerjaan, aturan-aturan, prosedur-prosedur yang akan digunakan untuk mengembangkan suatu sistem informasi.

Metodologi yang digunakan dalam analisis ini, yaitu:

1. *Functional Decomposition Methodologies*

Etologi ini melakukan pemecahan masalah dari sistem ke dalam subsistem-subsistem yang lebih kecil, sehingga lebih mudah dipahami, dirancang dan diterapkan. Alat (*tool*) yang digunakan adalah HIPO (*Hierarchy Plus Input Process-Output Process*), dengan menggunakan diagram *Visual Table of Content* (VTOC).

2. *Data Oriented Methodologies*

Menekankan pada karakteristik dari data yang akan diproses.

Alat yang digunakan adalah *Context Level Data Flow Diagram* (DFD).

3.2 Hasil Analisis

Berdasarkan data-data yang didapat, dapat diuraikan hasil analisis kebutuhan sistem sebagai berikut :

3.2.1 Analisis Kebutuhan Masukan

Pengolahan data masukan yang dibutuhkan dalam pengembangan sistem informasi transaksi prabayar dengan media *smart card* ini adalah sebagai berikut :

a. Data perusahaan

Kebutuhan data masukan meliputi : Nama perusahaan, alamat, kota, telepon, alamat email perusahaan, nama pemilik.

b. Data Administrator

Kebutuhan data masukan meliputi : Kode administrator, PIN administrator.

c. Data Pelanggan (*customers*)

Kebutuhan data masukan meliputi : nama pelanggan, alamat, kota, telepon, alamat email, pekerjaan, foto, jenis kelamin.

d. Data Operator

Kebutuhan data masukan meliputi : nama operator, alamat, kota, telepon, alamat email, foto, jenis kelamin, PIN, hak akses.

e. Data Barang (*item*)

Kebutuhan data masukan meliputi kode barang, nama, harga.

f. Data Suplier

Kebutuhan data masukan meliputi kode suplier, nama, alamat, kota, telepon.

g. Data Pembelian

Kebutuhan data masukan meliputi data suplier, data barang, kuantitas barang yang dibeli.

h. Data Penjualan

Kebutuhan data masukan meliputi *smart card*, *PIN smart card*, data barang, kuantitas barang yang dijual.

i. Data penambahan saldo pelanggan pada *smart card* (*reload*)

Kebutuhan data masukan meliputi *smart card*, *PIN smart card*, jumlah nominal penambahan saldo.

3.2.2 Analisis Kebutuhan Keluaran

Kebutuhan keluaran yang dibutuhkan dalam pengembangan sistem informasi transaksi prabayar ini meliputi informasi-informasi pelanggan, operator, barang, suplier, pembelian, penjualan, isi ulang, hutang piutang perusahaan.

3.2.3 Analisis Kebutuhan Antarmuka

Kebutuhan antarmuka yang diinginkan oleh pengguna berdasarkan hasil wawancara dengan pihak-pihak terkait, dibutuhkan antarmuka yang bersifat *user friendly* yaitu perangkat lunak yang dibuat harus dapat digunakan dengan mudah, nyaman dan meminimalisasi kemungkinan kesalahan, baik kesalahan *input*, proses *output*, dan disertai dengan *feedback* dari sistem, contohnya penanganan kesalahan memasukkan data.

Antarmuka yang dibutuhkan dalam sistem ini adalah :

1. Antarmuka halaman login.
2. Antarmuka halaman layanan pelanggan, yang meliputi personalisasi pelanggan, penjualan barang secara prabayar, pembelian barang dari supplier, pengisian ulang saldo kartu pelanggan.
3. Antarmuka halaman *setup* operator.
4. Antarmuka halaman *setup* barang.
5. Antarmuka halaman *setup* supplier.
6. Antarmuka halaman penggantian pin.
7. Antarmuka halaman konfigurasi jaringan.
8. Antarmuka halaman bantuan penggunaan aplikasi.

BAB IV

PERANCANGAN PERANGKAT LUNAK

4.1 Metode Perancangan

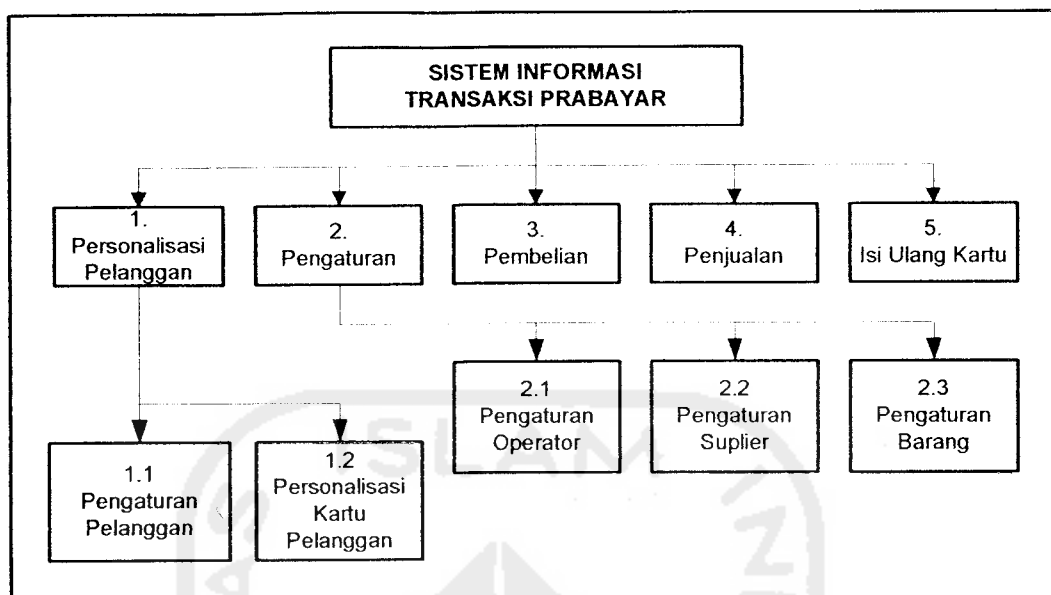
Perancangan perangkat lunak dilakukan dengan metode berorientasi pada aliran data, perancangan dimulai dengan perancangan diagram arus data (*data flow diagram*) beserta spesifikasi prosesnya, kamus data, aturan pengkodean, perancangan *memory mapping* pada *smart card* dan perancangan antarmuka dari sistem informasi transaksi prabayar.

4.2 Hasil Perancangan

Hasil perancangan yang didapat untuk membuat Sistem Informasi transaksi prabayar yaitu perancangan struktur pohon proses, perancangan diagram arus data DFD (*data flow diagram*) beserta spesifikasi prosesnya, kamus data, aturan pengkodean, perancangan *memory mapping* pada *smart card* dan perancangan antarmuka dari sistem informasi transaksi prabayar.

4.2.1 Struktur Pohon Proses

Struktur pohon proses akan sangat membantu dalam pembuatan suatu aplikasi. Melalui struktur pohon dapat diketahui proses-proses inti yang akan dilakukan beserta proses turunannya. Struktur pohon proses dapat dilihat pada gambar 4.1.



Gambar 4.1 Struktur Pohon Proses Sistem Informasi Transaksi Prabayar.

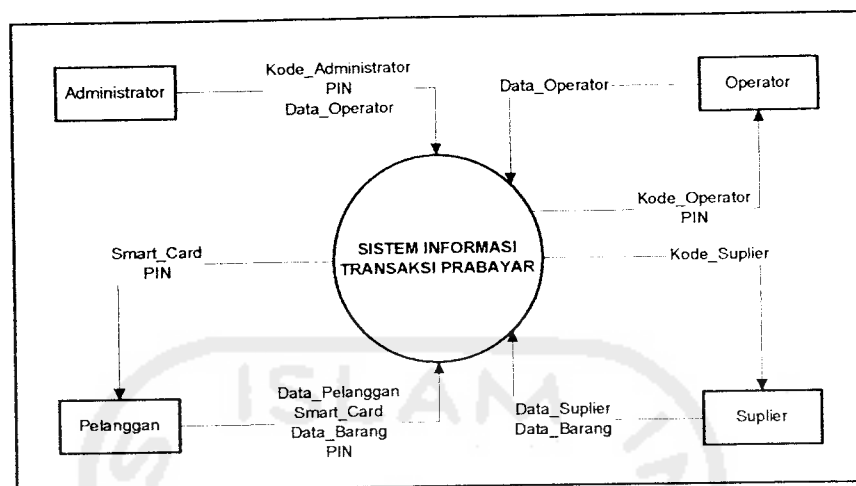
4.2.2 Diagram Arus Data DFD (*Data Flow Diagram*)

Data flow diagram adalah diagram yang memperlihatkan alir data antar proses dan tempat penyimpanan data. Proses, alir data, dan tempat penyimpanan data digambarkan dengan notasi tertentu.

Alir data digambarkan secara global pada diagram konteks. DFD pada tingkat yang lebih tinggi menggambarkan alir data dengan lebih detail [WAH02].

4.2.2.1 Diagram Konteks

Context Diagram (CD) adalah kasus khusus dari *Data Flow Diagram* (DFD) yaitu bagian dari DFD yang berfungsi memetakan model lingkaran yang direpresentasikan dengan lingkaran tunggal yang mewakili keseluruhan sistem. Diagram kontek dapat dilihat pada gambar 4.2

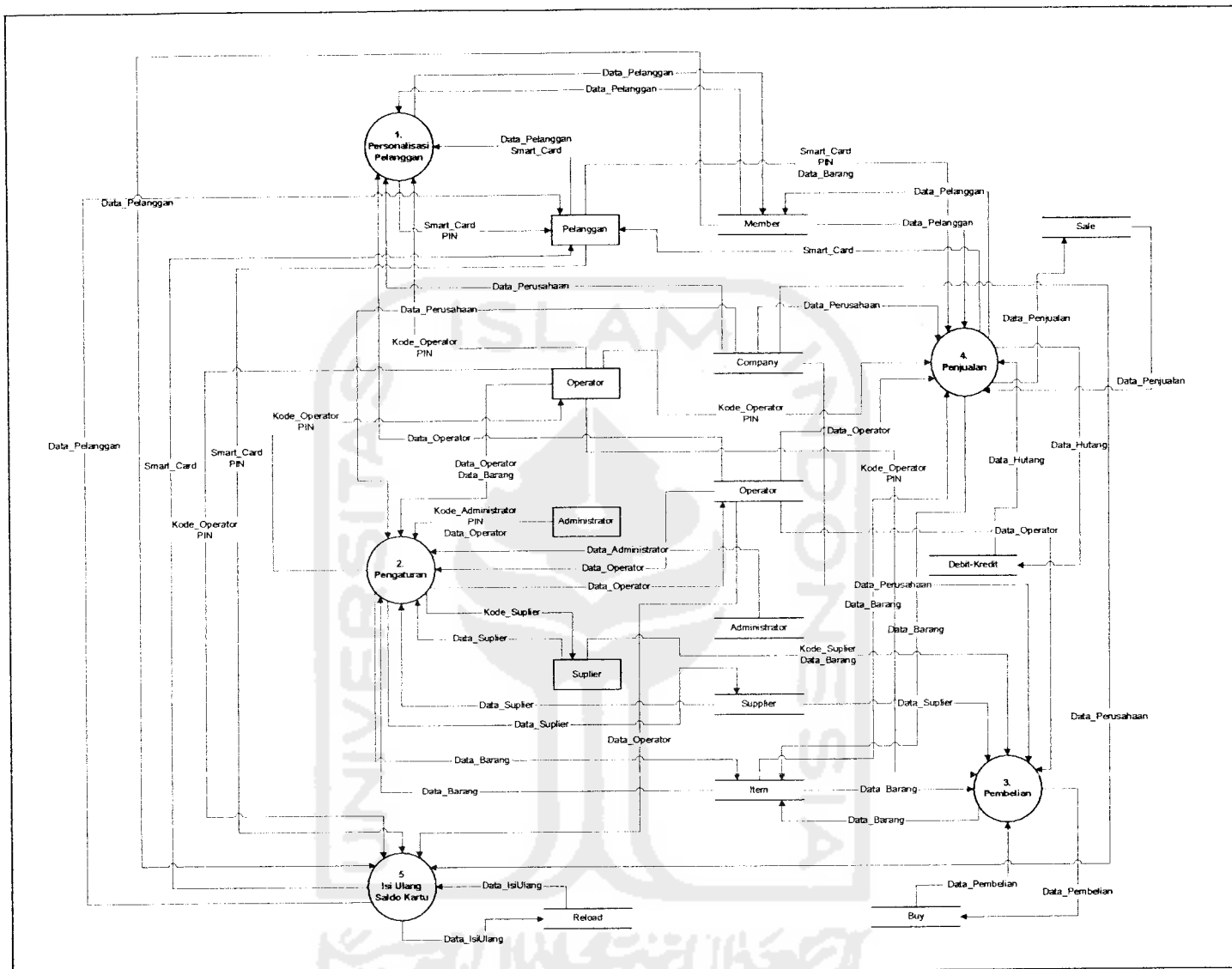


Gambar 4.2 Diagram Konteks Sistem Informasi Transaksi Prabayar

Penggunaan diagram konteks atau disebut DFD level 0, dimaksudkan untuk membantu menggambarkan arus data yang terjadi dalam sistem secara global. Diagram konteks menggambarkan hubungan data yang masuk ke sistem beserta sumber dan informasi yang dihasilkan.

4.2.2.2 Diagram Aliran Data Level 1 Sistem Informasi Transaksi Prabayar.

Pada DFD level 1 dari sistem informasi transaksi prabayar ini menjelaskan tentang penjabaran dari digram konteks sehingga lebih terperinci. Pada DFD level 1 ini proses dibagi menjadi 5 proses yang diuraikan secara terperinci, uraian proses tersebut adalah proses personalisasi pelanggan, pengaturan, pembelian, penjualan dan penambahan saldo pelanggan atau isi ulang kartu pelanggan. Diagram aliran data level 1 ini dapat dilihat pada gambar 4.3.

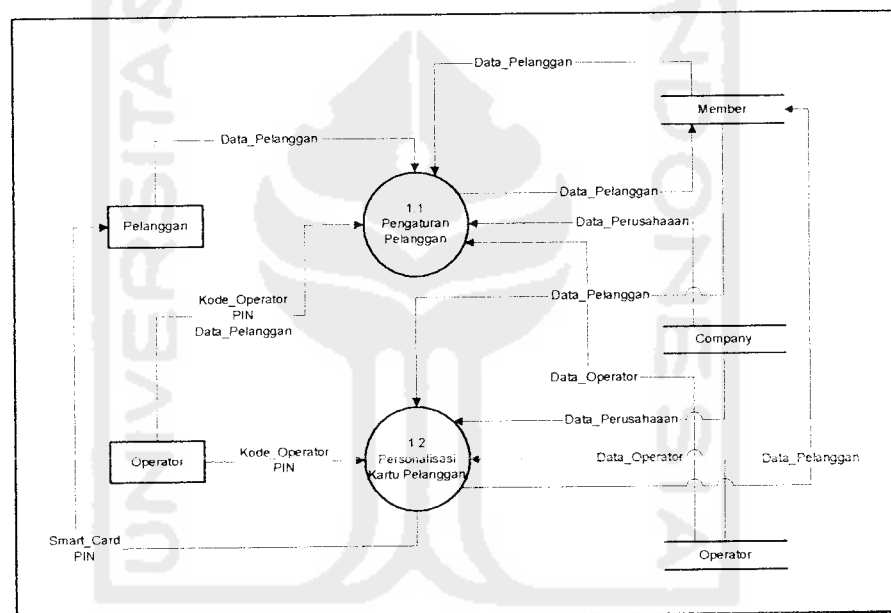


Gambar 4.3 DFD Level 1 Sistem Informasi Transaksi Prabayar

4.2.2.3 Diagram Aliran Data Level 2 dari Proses 1. Personalisasi

Pelanggan

Proses personalisasi pelanggan terdiri dari proses pengaturan pelanggan dan personalisasi kartu pelanggan, proses personalisasi pelanggan adalah pada saat konsumen datang ke suatu perusahaan, kemudian mendaftarkan diri sebagai pelanggan perusahaan tersebut.



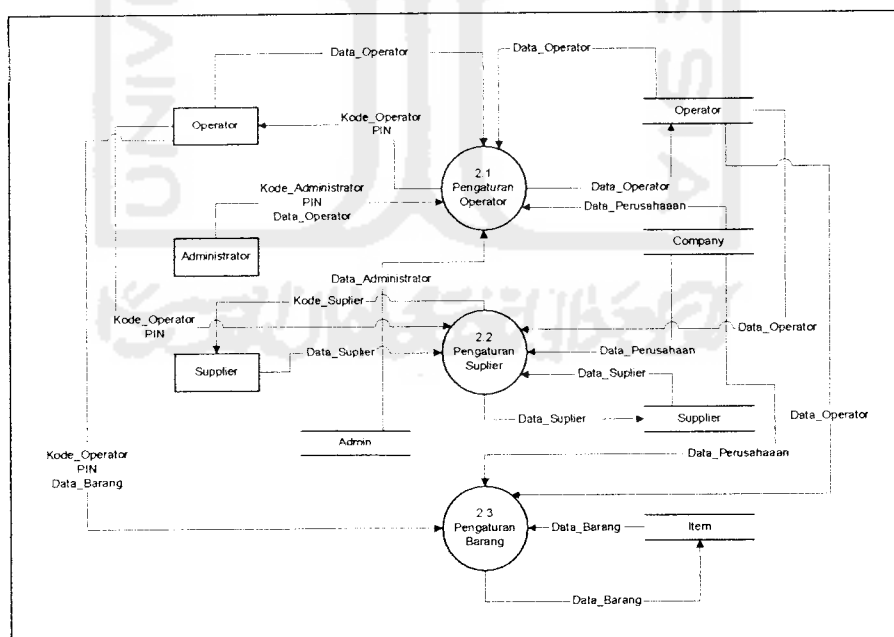
Gambar 4.4 Diagram Aliran Data Level 2 dari Proses 1. Personalisasi Pelanggan

Proses 1.1 pengaturan pelanggan adalah proses dimana saat pelanggan memberikan data personalnya kepada operator, kemudian operator memasukkan data tersebut kedalam *database*.

Proses 1.2 personalisasi kartu pelanggan adalah proses mengambil data pelanggan dari *database* kemudian dituliskan kedalam kartu (*smart card*).

4.2.2.4 Diagram Aliran Data Level 2 dari Proses 2. Pengaturan.

Proses 2. Pengaturan, terdiri dari 3 proses yaitu : proses pengaturan operator, pengaturan suplier, dan pengaturan barang. Proses pengaturan adalah proses memasukkan, pengubahan, penghapusan, dan melihat data yang ada didalam *database*. Pada proses pengaturan operator dilakukan oleh administrator, sehingga administrator bertanggung jawab penuh akan kerja operator didalam sistem. Pengaturan suplier dan barang dilakukan oleh operator. DFD level 2 ini dapat dilihat pada gambar 4.5



Gambar 4.5 Diagram Aliran Data Level 2 dari Proses 2. Pengaturan.

4.2.3 Spesifikasi Proses Sistem Informasi Transaksi Prabayar.

Spesifikasi proses ini berguna untuk menjelaskan secara terperinci dari masing-masing proses, spesifikasi proses terdiri dari logika proses, aliran data (data masuk dan data keluar), dan algoritma dari proses tersebut.

Tabel 4.1. Spesifikasi Proses 1. 1 Pengaturan Pelanggan

Nama Proses	1.1. Pengaturan Pelanggan Proses pengaturan pelanggan ini dilakukan oleh operator, yang memiliki hak akses akan layanan pengaturan pelanggan dan bertugas menangani pemasukkan, pengubahan, penghapusan, dan melihat data personal pelanggan.	
Logika Proses	Pengaturan pelanggan adalah proses mengolah data pelanggan yang meliputi : <ul style="list-style-type: none"> ▪ Input data : Memasukkan data pelanggan (registrasi pelanggan). ▪ Ubah data : Mengubah data pelanggan. ▪ Hapus data : Menghapus data pelanggan. ▪ Lihat data : Melihat data pelanggan. 	
Aliran Data	Data Masuk	Data pelanggan dari pelanggan yang menuju proses 1.1 pengaturan pelanggan.
		Data pelanggan dari operator yang menuju proses 1.1 pengaturan pelanggan.
		Data operator (Kode dan PIN) dari operator yang menuju proses 1.1 pengaturan pelanggan.
		Data pelanggan dari tabel member yang menuju proses 1.1 pengaturan pelanggan.
		Data perusahaan dari tabel company yang menuju proses 1.1 pengaturan pelanggan.
		Data operator dari tabel operator yang menuju proses 1.1 pengaturan pelanggan.

	Data Keluar	Data pelanggan dari proses 1.1 pengaturan pelanggan menuju tabel pelanggan.
Algoritma	<ul style="list-style-type: none"> ▪ Untuk dapat mengakses pelayanan pengaturan pelanggan sistem akan meminta kode dan pin operator, kemudian membaca data operator pada tabel operator dan data perusahaan pada tabel company. ▪ Pelanggan akan memberikan data personalnya kepada operator. ▪ Operator memasukkan data pelanggan kedalam tabel member. ▪ Untuk mengubah, menghapus dan melihat data pelanggan, sistem akan membaca data pelanggan dalam tabel member, kemudian setelah proses yang diinginkan dilakukan maka data pelanggan dimasukkan kembali ke dalam tabel member 	

Tabel 4.2. Spesifikasi Proses 1.2 Personalisasi Kartu Pelanggan.

Nama Proses	1.2 Personalisasi Kartu Pelanggan Proses personalisasi kartu ini dilakukan oleh operator yang menangani registrasi pelanggan baru, proses ini terjadi saat operator melakukan proses penulisan data pelanggan pada kartu.	
Logika Proses	Personalisasi kartu adalah proses membaca dan menuliskan data pelanggan dari tabel member kedalam kartu pelanggan. Dimana data pelanggan yang dituliskan kedalam kartu adalah kode pelanggan, kode perusahaan, nama pelanggan, PIN yang sudah terenkripsi, saldo pelanggan.	
Aliran Data	Data Masuk	Data pelanggan dari tabel member menuju proses 1.2 personalisasi kartu pelanggan.
		Data operator (kode dan PIN) dari operator menuju proses 1.2 personalisasi kartu pelanggan.

		Data perusahaan dari tabel company menuju proses 1.2 personalisasi kartu pelanggan.
		Data operator dari tabel operator menuju proses 1.2 personalisasi kartu pelanggan.
	Data Keluar	<p>Data pelanggan (PIN, <i>smart card</i>) dari proses 1.2 personalisasi kartu pelanggan menuju pelanggan</p> <p>PIN adalah <i>personal identity number</i> untuk pelanggan yang berguna untuk pemakaian <i>smart card</i> dalam bertransaksi diperusahaan yang bersangkutan.</p> <p><i>Smart Card</i> adalah bukti bahwa pelanggan sudah teregistrasi dan berstatus aktif untuk menggunakan kartu jika debit $\neq 0$.</p>
		Data pelanggan dari proses 1.2 personalisasi kartu pelanggan menuju tabel member
Algoritma	<p>Jika proses personalisasi kartu pelanggan dilakukan maka :</p> <ul style="list-style-type: none"> ▪ Operator memasukkan data operator (kode dan pin) untuk bisa mengakses sistem, agar dapat melayani personalisasi pelanggan. ▪ Membaca data operator dan data perusahaan pada tabel operator dan tabel company. ▪ Membaca data pelanggan pada tabel member. ▪ Mencari data pelanggan yang diinginkan, kemudian dilakukan mengenkripsian PIN, setelah itu semua data tersebut sudah siap ditulis ke dalam kartu. <p>Menyerahkan kartu kepada pelanggan disertai PIN.</p>	

Tabel 4.3 Spesifikasi Proses 2.1 Pengaturan Operator.

Nama Proses	2.1 Pengaturan Operator Proses pengaturan operator ini dilakukan oleh administrator sistem, yang bertugas melakukan pemasukkan, pengubahan, penghapusan, dan melihat data operator.	
Logika Proses	Pengaturan Operator adalah proses mengolah data operator yang meliputi : <ul style="list-style-type: none"> ▪ Input data : Memasukkan data operator (registrasi operator). ▪ Ubah data : Mengubah data operator. ▪ Hapus data : Menghapus data operator. ▪ Lihat data : Melihat data operator. 	
Aliran Data	Data Masuk	Data administrator (kode dan PIN) dari administrator menuju proses 2.1 pengaturan operator.
		Data operator dari administrator menuju proses 2.1 pengaturan operator.
		Data operator dari operator menuju proses 2.1 pengaturan operator
		Data operator dari tabel operator menuju proses 2.1 pengaturan operator.
		Data perusahaan dari tabel company menuju proses 2.1 pengaturan operator.
		Data administrator dari tabel admin menuju proses 2.1 pengaturan operator
	Data Keluar	Data operator dari proses 2.1 pengaturan operator menuju tabel operator.
		Data operator (kode, PIN) dari proses 2.1 pengaturan operator yang menuju operator PIN berguna bagi operator untuk bisa mengakses kedalam sistem transaksi prabayar.

Algoritma	<ul style="list-style-type: none"> ▪ Untuk mengakses layanan pengaturan operator, sistem membutuhkan kode dan PIN dari administrator, kemudian membaca data administrator pada tabel admin dan data perusahaan pada tabel company. ▪ Jika proses input data operator dilakukan, maka masukkan data operator ke dalam tabel operator. ▪ Jika proses ubah data operator dilakukan, maka cari data operator pada tabel operator, kemudian ubah data operator tersebut, lalu masukkan kembali data operator yang sudah diubah kedalam tabel operator. ▪ Jika proses hapus data operator dilakukan, maka cari data operator pada tabel operator, kemudian hapus data operator tersebut. ▪ Jika proses lihat data operator dilakukan, maka cari seluruh data operator pada tabel operator.
-----------	---

Tabel 4.4 Spesifikasi Proses 2.2 Pengaturan Suplier.

Nama Proses	2.2 Pengaturan Suplier Proses pengaturan suplier ini dilakukan oleh operator, yang bertugas melakukan pemasukkan, pengubahan, penghapusan dan melihat data suplier.	
Logika Proses	Pengaturan suplier adalah proses mengolah data suplier yang meliputi : <ul style="list-style-type: none"> ▪ Input data : Memasukkan data suplier. ▪ Ubah data : Mengubah data suplier. ▪ Hapus data : Menghapus data suplier. ▪ Lihat data : Melihat data suplier. 	
Aliran Data	Data Masuk	Data suplier dari suplier yang menuju proses 2.2 pengaturan suplier.
		Data suplier dari tabel supplier ke proses 2.2 pengaturan suplier.

		Data operator (kode dan PIN) dari operator yang menuju proses 2.2 pengaturan supplier.
		Data perusahaan dari tabel company yang menuju proses 2.2 pengaturan supplier.
	Data Keluar	Data supplier dari proses 2.2 pengaturan supplier menuju tabel supplier.
		Data supplier (kode) dari proses 2.2 pengaturan supplier menuju supplier
Algoritma	<ul style="list-style-type: none"> ▪ Untuk dapat mengakses layanan pengaturan supplier sistem membutuhkan kode dan PIN dari operator, kemudian membaca data operator pada tabel operator dan data perusahaan pada tabel company. ▪ Jika proses input data supplier dilakukan, maka masukkan data supplier baru ke dalam tabel supplier. ▪ Jika proses ubah data supplier dilakukan, maka cari data supplier pada tabel supplier, lalu ubah data supplier tersebut, kemudian masukkan kembali data supplier yang sudah diubah kedalam tabel supplier. ▪ Jika proses hapus data supplier dilakukan, maka cari data supplier pada tabel supplier, kemudian hapus data supplier tersebut. ▪ Jika proses lihat data supplier dilakukan, maka cari seluruh data supplier pada tabel supplier. 	

Tabel 4.5 Spesifikasi Proses 2.3 Pengaturan Barang.

Nama Proses	<p>2.3 Pengaturan Barang</p> <p>Proses pengaturan barang ini dilakukan oleh operator yang bertugas melakukan pemasukkan, pengubahan, penghapusan dan melihat data barang.</p>
Logika Proses	<p>Pengaturan Barang adalah proses mengolah data barang yang meliputi :</p> <ul style="list-style-type: none"> ▪ Input data : Memasukkan data barang. ▪ Ubah data : Mengubah data barang.

	<ul style="list-style-type: none"> ▪ Hapus data : Menghapus data barang. ▪ Lihat data : Melihat data barang. 	
Aliran Data	Data Masuk	Data barang yang berasal dari operator menuju proses 2.3 pengaturan barang
		Data operator (kode dan PIN) dari operator yang menuju proses 2.3 pengaturan barang.
		Data perusahaan dari tabel company yang menuju proses 2.3 pengaturan barang
		Data barang dari tabel item yang menuju proses 2.3 pengaturan barang
		Data operator dari tabel operator yang menuju proses 2.3 pengaturan barang.
	Data Keluar	Data barang yang berasal dari proses 2.3 pengaturan barang menuju tabel item.
Algoritma	<ul style="list-style-type: none"> ▪ Untuk dapat mengakses layanan pengaturna barang sistem membutuhkan kode dan Pin operator, kemudian membaca data operator pada tabel operator dan data perusahaan pada tabel company. ▪ Jika proses input data barang dilakukan, maka masukkan data barang baru ke dalam tabel item. ▪ Jika proses ubah data barang dilakukan, maka cari data barang pada tabel item, lalu ubah data barang tersebut, kemudian masukkan kembali data barang yang sudah diubah kedalam tabel item. ▪ Jika proses hapus data barang dilakukan, maka cari data barang pada tabel item, kemudian hapus data barang tersebut. ▪ Jika proses lihat data barang dilakukan, maka cari seluruh data barang pada tabel item. 	

Tabel 4.6 Spesifikasi Proses 3. Pembelian

Nama Proses	3. Pembelian Proses pembelian barang ini dilakukan pada saat perusahaan akan melakukan pengolahan data pembelian barang dari supplier.	
Logika Proses	Pembelian barang adalah proses mengolah data pembelian barang perusahaan yang dibeli dari supplier	
Aliran Data	Data Masuk	Data operator (kode dan PIN) dari operator menuju proses 3. pembelian.
		Data supplier (kode) dari supplier yang menuju proses 3.pembelian.
		Data barang dari supplier yang menuju proses 3.pembelian
		Data perusahaan dari tabel company yang menuju proses 3.pembelian
		Data pembelian dari tabel buy yang menuju proses 3. pembelian.
		Data barang dari tabel item yang menuju proses 3. pembelian.
		Data operator dari tabel operator yang menuju proses 3. pembelian.
	Data Keluar	Data pembelian dari proses 3. pembelian yang menuju tabel buy.
		Data barang dari proses 3. pembelian yang menuju tabel item.
Algoritma	Jika proses pembelian barang dilakukan maka : <ul style="list-style-type: none"> ▪ Untuk dapat mengakses layanan pembelian barang sistem membutuhkan kode dan PIN dari operator, kemudian membaca data operator pada tabel operator dan data perusahaan pada tabel company ▪ Masukkan data barang yang dibeli kemudian baca data barang pada tabel item ▪ Masukkan data supplier kemudian baca data supplier 	

	<p>pada tabel supplier</p> <ul style="list-style-type: none"> ▪ Masukkan data pembelian pada tabel buy
--	---

Tabel 4.7 Spesifikasi Proses Penjualan

Nama Proses	<p>4. Penjualan</p> <p>Proses ini ditangani oleh operator yang bertugas mengolah data transaksi penjualan barang secara prabayar.</p>	
Logika Proses	<p>Proses dimana pelanggan melakukan transaksi pembelian barang dengan menggunakan <i>smart card</i> secara prabayar.</p>	
Aliran Data	Data Masuk	Data operator (kode dan PIN) dari operator yang menuju proses 4. penjualan.
		Data barang dari pelanggan yang menuju proses 4. penjualan.
		Data barang dari tabel item yang menuju proses 4. penjualan.
		Data penjualan dari tabel sale yang menuju proses 4. penjualan.
		Data perusahaan dari tabel company yang menuju proses 4. penjualan.
		Data pelanggan (PIN) dan smart card dari pelanggan yang menuju proses 4. penjualan.
		Data hutang dari tabel debit_kredit yang menuju proses 4. penjualan.
		Data operator dari tabel operator yang menuju proses 4. penjualan.
		Data pelanggan dari tabel member yang menuju proses 4. penjualan.
	Data Keluar	Data pelanggan dari proses 4. penjualan yang menuju tabel member.
		Smart card dari proses 4. penjualan yang menuju pelanggan

		Data barang dari proses 4. penjualan yang menuju tabel item.
		Data penjualan dari proses 4. penjualan yang menuju tabel sale.
		Data hutang dari proses 4. penjualan yang menuju tabel debit_kredit.
Algoritma	<p>Jika proses penjualan dilakukan maka :</p> <ul style="list-style-type: none"> ▪ Untuk dapat mengakses layanan penjualan sistem membutuhkan kode dan PIN operator, kemudian membaca data operator pada tabel operator, dan data perusahaan pada tabel company. ▪ Masukkan <i>smart card</i> pelanggan beserta pin kemudian baca data pelanggan pada <i>smart card</i> dan cek data pelanggan pada tabel member ▪ Baca data perusahaan pada tabel company ▪ Masukkan data barang yang akan dibeli kemudian cek data barang pada tabel item ▪ Masukkan data penjualan kedalam tabel sale ▪ Bila terjadi hutang / piutang maka baca data_hutang pada tabel debit_kredit, kemudian <i>update</i> data_hutang setelah itu simpan kembali pada tabel debit_kredit. 	

Tabel 4.8 Spesifikasi Proses 5. Isi Ulang Saldo Kartu

Nama Proses	<p>5. Isi Ulang Saldo Kartu</p> <p>Proses ini ditangani oleh operator yang bertugas mengolah data isi ulang saldo pelanggan.</p>	
Logika Proses	<p>Proses dimana pelanggan melakukan transaksi penambahan saldo untuk bertransaksi secara parabayar.</p>	
Aliran Data	Data Masuk	Data pelanggan (PIN) dan smart card dari pelanggan yang menuju proses 5. isi ulang saldo kartu.

		Data operator (Kode dan PIN) dari operator yang menuju proses 5. isi ulang saldo kartu.
		Data isi ulang dari tabel reload menuju proses 5. isi ulang saldo kartu.
		Data pelanggan dari tabel member yang menuju proses 5. isi ulang saldo kartu.
		Data perusahaan dari tabel company menuju proses 5. isi ulang saldo kartu.
		Data operator dari tabel operator yang menuju proses 5. isi ulang saldo kartu.
	Data Keluar	Smart card dari proses 5. isi ulang saldo kartu menuju pelanggan
		Data pelanggan dari proses 5. isi ulang saldo kartu menuju tabel member.
		Data isi ulang dari proses 5. isi ulang menuju tabel reload.
Algoritma	<p>Jika proses isi ulang dilakukan maka :</p> <ul style="list-style-type: none"> ▪ Untuk dapat mengakses layanan isi ulang sistem membutuhkan kode dan PIN operator, kemudian membaca data operator pada tabel operator dan data perusahaan pada tabel company. ▪ Masukkan <i>smart card</i> beserta pin pelanggan kemudian baca data pelanggan pada kartu dan cek data pelanggan pada tabel member ▪ Masukkan jumlah nominal pengisian <i>point</i>, kemudian <i>update</i> data pelanggan didalam kartu dan tabel member. 	

4.2.4 Kamus Data

Kamus data berguna untuk merepresentasikan atau menerangkan data-data yang terdapat didalam proses.

Tabel 4.9 Kamus data

Data Pelanggan	Kode pelanggan, nama, alamat, kota, telepon, email, tanggal registrasi, status, jenis kelamin, pekerjaan, foto	
Kode pelanggan	0 { karakter valid_1 } 9	Kode pelanggan
Nama	0 { karakter valid } 30	Nama pelanggan
Alamat	0 { karakter valid } 50	Alamat pelanggan
Kota	0 { karakter valid } 25	Kota pelanggan
Telepon	0 { karakter valid_1 } 20	Telepon pelanggan
Jenis kelamin	Enumerasi Pria / Wanita	Jenis kelamin pelanggan (Pria atau Wanita)
Status	Enumerasi Aktif / Non aktif	Status pelanggan (Aktif atau Non aktif)
Pekerjaan	0 { karakter valid } 30	Pekerjaan pelanggan
Foto	[mediumBLOB]	Foto pelanggan
Tanggal registrasi	Format tanggal (yyyy-mm-dd)	Tanggal registrasi
Email	Format email <u>xxx@xxx.xxx</u> <u>xxx@xxx.xx.xx</u>	Alamat email pelanggan
Data Operator	Kode operator, nama, alamat, kota, telepon, email, tanggal registrasi, PIN, status, jenis kelamin, foto, akses pembelian, akses penjualan, akses isi ulang, akses personalisasi, akses atur barang	
Kode operator	0 { karakter valid_1 } 9	Kode operator
Nama	0 { karakter valid } 30	Nama operator

Alamat	0 { karakter valid } 50	Alamat operator
Kota	0 { karakter valid } 25	Kota operator
Telepon	0 { karakter valid_1 } 20	Telepon operator
Jenis kelamin	Enumerasi Pria / Wanita	Jenis kelamin pelanggan (Pria atau Wanita)
Status	Enumerasi Aktif / Non aktif	Status pelanggan (Aktif atau Non aktif)
Foto	[mediumBLOB]	Foto operator
Tanggal registrasi	Format tanggal (yyyy-mm-dd)	Tanggal registrasi
Pin	0 { karakter valid_1 } 6	Pin operator yang berguna untuk mengakses sistem
Email	Format email <u>xxx@xxx.xxx</u> xxx@xxx.xx.xx	Alamat Email operator
Akses pembelian	Enumerasi Granted / Denied	Hak akses, berguna untuk pengaturan hak akses (pembelian)
Akses penjualan	Enumerasi Granted / Denied	Hak akses, berguna untuk pengaturan hak akses (penjualan)
Akses isi ulang	Enumerasi Granted / Denied	Hak akses, berguna untuk pengaturan hak akses (isi ulang)
Akses personalisasi	Enumerasi Granted / Denied	Hak akses, berguna untuk pengaturan hak akses (personalisasi)
Akses atur barang	Enumerasi Granted / Denied	Hak akses, berguna untuk pengaturan hak akses (pengaturan barang)
Data Perusahaan	Kode perusahaan, nama, alamat, kota, telepon, email, pemilik, tanggal registrasi, status	
Kode perusahaan	0 { karakter valid_1 } 9	Kode perusahaan

Nama	0 { karakter valid } 30	Nama perusahaan
Alamat	0 { karakter valid } 50	Alamat perusahaan
Kota	0 { karakter valid } 25	Kota perusahaan
Telepon	0 { karakter valid_1 } 20	Telepon perusahaan
Pemilik	0 { karakter valid } 30	Pemilik perusahaan
Email	Format email <u>xxx@xxx.xxx</u> <u>xxx@xxx.xx.xx</u>	Alamat email perusahaan
Tanggal registrasi	Format tanggal (yyyy-mm-dd)	Tanggal registrasi
Status	Enumerasi Aktif / Non aktif	Status perusahaaan (Aktif atau Non aktif)
Data Barang	Kode barang, nama, harga, stok	
Kode barang	Barcode tipe EAN 13 (13 digit)	Kode barang
Nama barang	0 { karakter valid } 30	Nama barang
Stok barang	0 {karakter valid_1} 9	Jumlah stok barang
Harga barang	Format (x.xxx.xxx)	Harga barang
Data Suplier	Kode suplier, nama, alamat, kota, telepon	
Kode suplier	0 { karakter valid_1} 9	Kode suplier
Nama suplier	0 { karakter valid } 30	Nama suplier
Alamat	0 { karakter valid } 50	Alamat suplier
Kota	0 { karakter valid } 25	Kota suplier
Telepon	0 { karakter valid_1 } 20	Telepon suplier
Data Hutang	Kode perusahaan debit, kode perusahaan kredit, jumlah hutang	
Kode perusahaan debit	0 { karakter valid_1} 9	Kode perusahaan yang mempunyai piutang
Kode perusahaan	0 { karakter valid_1} 9	Kode perusahaan yang

kredit		mempunyai hutang
Jumlah hutang	Format (x.xxx.xxx)	Jumlah nominal hutang
Data Pembelian	No.Nota, tanggal, total	
Tanggal	Format tanggal (yyyy-mm-dd)	Tanggal pembelian
No.Nota	0 { karakter valid_1 } 9	No Nota transaksi pembelian
Total	Format (x.xxx.xxx)	Total nominal transaksi
Data Penjualan	No.Nota, tanggal, total	
No nota	0 { karakter valid_1 } 15	No nota penjualan
Tanggal	Format tanggal (yyyy-mm-dd)	Tanggal pembelian
Total	Format (x.xxx.xxx)	Total nominal transaksi
Data Administrator	Kode administrator, nama, alamat, kota,telepon, email, tanggal registrasi, PIN, status, jenis kelamin, foto	
Kode administrator	0 { karakter valid_1 } 9	Kode administrator
Nama	0 { karakter valid } 30	Nama administrator
Alamat	0 { karakter valid } 50	Alamat administrator
Kota	0 { karakter valid } 25	Kota administrator
Telepon	0 { karakter valid_1 } 20	Telepon administrator
Jenis kelamin	Enumerasi Pria / Wanita	Jenis kelamin administrator (Pria atau Wanita)
Status	Enumerasi Aktif / Non aktif	Status administrator (Aktif atau Non aktif)
Foto	[mediumBLOB]	Foto administrator
Tanggal registrasi	Format tanggal (yyyy-mm-dd)	Tanggal registrasi
Pin	0 { karakter valid_1 } 6	Pin administrator yang berguna untuk mengakses sistem

Email	Format email <u>xxx@xxx.xxx</u> <u>xxx@xxx.xx.xx</u>	Alamat Email administrator
Keterangan :		
Karakter valid	[A-Z a-z 0-9]	
Karakter valid_1	[0-9]	

4.2.5 Aturan Pengkodean

Tabel 4.10 Pengkodean perusahaan

Pengkodean ini berguna sebagai aturan pengkodean perusahaan (*company id*).

XXX	XXX	XXX
212	000	001
Kode Perusahaan	Const	Index (Identifikasi Perusahaan)
Maksimal	212000999	

Tabel 4.11 Pengkodean operator

Pengkodean ini berguna sebagai aturan pengkodean operator (*operator id*).

XXX	XXX	XXX
103	001	001
Kode Operator	Identifikasi Perusahaan	Index
Maksimal	103999999	

Tabel 4.12 Pengkodean pelanggan

Pengkodean ini berguna sebagai aturan pengkodean pelanggan (*member id*).

XXX	XXXXXX
001	000001
Identifikasi Perusahaan	Index
Maksimal	999999999

Tabel 4.13 Pengkodean administrator.

Pengkodean ini berguna sebagai aturan pengkodean administrator (*administrator id*).

XXX	XXX	XXX
007	001	001
Kode Administrator	Identifikasi Perusahaan	Index
Maksimal	007999999	

4.2.6 Pengalamatan Memori *Smart Card*

Smart Card SLE 4428 mempunyai 1024 x 8 bit EEPROM dan *protection byte*. Memori harus diproteksi menggunakan fungsi autentifikasi yang digunakan pada saat menuliskan data pada kartu.


```

0x02F0 | 0752 - 0767 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0300 | 0768 - 0783 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0310 | 0784 - 0799 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0320 | 0800 - 0815 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0330 | 0816 - 0831 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0340 | 0832 - 0847 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0350 | 0848 - 0863 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0360 | 0864 - 0879 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0370 | 0880 - 0895 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0380 | 0896 - 0911 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x0390 | 0912 - 0927 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x03A0 | 0928 - 0943 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x03B0 | 0944 - 0959 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x03C0 | 0960 - 0975 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x03D0 | 0976 - 0991 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x03E0 | 0992 - 1007 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x03F0 | 1008 - 1023 : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

```

Keterangan :



= Kode pemegang kartu. (9 byte)



= Nama pemegang kartu. (20 byte)



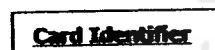
= Hasil enkripsi PIN pelanggan dengan key PSC. (24 byte)



= Hasil enkripsi PSC dengan secret key. (16 byte)



= Total Saldo pemegang kartu. (10 byte)



= Identitas Kartu. (13 byte)



= Kode perusahaan. (3 byte)



= Jumlah saldo pada perusahaan terkait. (10 byte)



= Panjang record. (1 byte)



= Programmable Security Code (PSC)

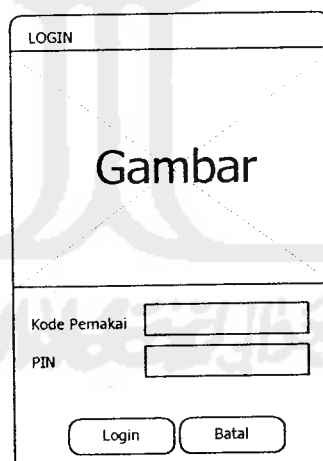
_____ = Protection byte = True

4.2.7 Rancangan Kebutuhan Antarmuka (*Interface*)

Kebutuhan antarmuka (*interface*) dirancang sedemikian rupa guna memudahkan pengguna untuk menjalankan program aplikasi sehingga antara program dan pengguna dapat berinteraksi dengan baik. Tampilan antar muka terdiri dari :

1. Rancangan antarmuka halaman login.

Rancangan antarmuka halaman login bagi pengguna sistem transaksi prabayar akan terlihat seperti gambar 4.6. Pada halaman login ini pengguna sistem diminta untuk memasukkan kode pemakai dan PIN.



LOGIN

Gambar

Kode Pemakai

PIN

Login Batal

Gambar 4.6 Rancangan antarmuka halaman login

2. Rancangan antarmuka halaman konfigurasi jaringan.

Rancangan antarmuka halaman konfigurasi jaringan ini berguna untuk menghubungkan *client* dengan *server*. Rancangan akan terlihat seperti pada gambar 4.7.

The image shows a software window titled "Client" with a standard Windows-style title bar (minimize, maximize, close buttons). The main content area is titled "Konfigurasi" and is divided into two sections: "Server" and "Client".

- Server Section:** Contains three input fields. The first is "IP Server", represented by four adjacent boxes for each digit. The second is "Kanal Server", represented by a single box. The third is "Database", represented by a single box.
- Client Section:** Contains three input fields. The first is "Kode Perusahaan", represented by a single box. The second is "Kunci Umum", represented by a single box. The third is "Konfirmasi", represented by a single box.

Below the input fields, there is a warning message: "Konfigurasi yang tidak tepat akan berakibat komputer tidak dapat terhubung dengan server". At the bottom of the window, there are two buttons: "Ubah" (Change) and "Tutup" (Close).

Gambar 4.7 Rancangan antarmuka halaman konfigurasi jaringan

3. Rancangan antarmuka halaman pengaturan operator.

Rancangan antarmuka halaman pengaturan operator ini berguna untuk menangani proses pengaturan operator, yaitu proses penambahan, pengubahan, penghapusan, dan melihat data operator. Dalam proses pengaturan operator ini adalah hak akses dari administrator. Rancangan akan terlihat seperti pada gambar 4.8.

Pengaturan Operator

Operator

Kode Operator

☐ Foto

Nama

Alamat Tinggal

Kota

Telepon

Pekerjaan

Email

Jenis Kelamin ☐ Pria ☐ Wanita

Nilai Baku

☐ Status ☐ Aktif ☐ Non Aktif

☐ PIN

Konfirmasi

Hak Akses

☐ Pembelian ☐ Personalisasi

☐ Penjualan

☐ Isi Ulang ☐ Pengaturan Barang

Kode	Nama	Status

Tambah Hapus Ubah Tutup

Gambar 4.8 Rancangan antarmuka halaman pengaturan operator.

4. Rancangan antarmuka halaman pengaturan barang.

Rancangan antarmuka halaman pengaturan barang ini, berguna untuk proses pengaturan barang yang terdiri dari penambahan, pengubahan, penghapusan, dan melihat data barang, halaman ini dijalankan oleh operator perusahaan. Rancangan ini akan terlihat pada gambar 4.9

Pengaturan Barang

Barang

Data

☒ Kode Barang

☐ Nama Barang

☐ Harga Barang

Barcode EAN-13

No.	Kode Barang	Nama Barang	Harga Satuan (Rp)	Stok

Total Barang : 0 Item

Tambah Ubah Hapus Tutup

Gambar 4.9 Rancangan antarmuka halaman pengaturan barang.

5. Rancangan antarmuka halaman pengaturan supplier.

Rancangan antarmuka halaman pengaturan supplier ini berguna untuk proses pengaturan supplier, yang terdiri dari penambahan, pengubahan, penghapusan, dan melihat data supplier. Rancangan ini dapat dilihat pada gambar 4.10.

Pengaturan Penyalur

Penyalur

Kode Penyalur

Nama

Alamat

Kota

Telepon

Kode	Nama

Tambah Hapus Ubah Tutup

Gambar 4.10 Rancangan antarmuka halaman pengaturan suplier.

6. Rancangan antarmuka halaman pembelian.

Rancangan antarmuka halaman pembelian ini berguna untuk menangani proses pembelian barang oleh perusahaan dari suplier (penyalur), rancangan dapat dilihat pada gambar 4.11.

Layanan Pelanggan [X]

Informasi Penyalur

Kode Penyalur

Nama Penyalur

Penjualan | Pembelian | Isi Ulang | Personalisasi

No. Transaksi **Tanggal Transaksi**

Item Barang

Kode Barang

Nama Barang

Jumlah

BARCODE EAN 13

No.	Kode Barang	Nama Barang	Harga	Jumlah	Sub Total

Terbilang :

Masukkan Smart Card

Gambar 4.11 Rancangan antarmuka halaman pembelian.

7. Rancangan antarmuka halaman penjualan.

Rancangan antarmuka halaman penjualan ini berguna untuk menangani proses penjualan barang kepada pelanggan secara prabayar yang menggunakan media *smart card*. Pelanggan akan memberikan *smart card* dan PIN kepada sistem, setelah data pelanggan *valid* maka proses dapat dilakukan. Rancangan akan terlihat seperti gambar 4.12.

Layanan Pelanggan

Informasi Kartu

Kode Pelanggan

Nama Pelanggan

Saldo Rp.

FOTO

Verifikasi PIN

Kesempatan Verifikasi PIN 8 kali

Penjualan | Pembelian | Isi Ulang | Personalisasi

No. Transaksi **Tanggal Transaksi**

Item Barang

Kode Barang

Nama Barang

Jumlah

Barcode EAN 13

No.	Kode Barang	Nama Barang	Harga	Jumlah	Sub Total

Terbilang :

Masukkan Smart Card

Gambar 4.12 Rancangan antarmuka halaman penjualan.

8. Rancangan antarmuka halaman personalisasi pelanggan.

Rancangan antarmuka halaman personalisasi pelanggan ini berguna untuk menangani proses pengaturan pelanggan dan personalisasi kartu pelanggan. Proses pengaturan pelanggan terdiri dari penambahan, pengubahan, penghapusan data pelanggan, sedangkan proses personalisasi pelanggan adalah proses dimana saat operator akan menulis data pelanggan kedalam *smart card*. Rancangan akan terlihat seperti pada gambar 4.13

Gambar 4.13 Rancangan antarmuka halaman personalisasi pelanggan

9. Rancangan antarmuka halaman isi ulang saldo pelanggan.

Rancangan antarmuka halaman isi ulang saldo pelanggan ini berguna untuk menangani proses pengisian ulang saldo kartu pelanggan. Dalam proses ini pelanggan harus memberikan *smart card* dan PIN kepada sistem untuk dapat melakukan proses penambahan saldo pada kartu (*smart card*).

Rancangan antarmuka halaman ini akan terlihat seperti pada gambar 4.14.

Layanan Pelanggan

Informasi Kartu

☐

Kode Pelanggan

☐

Nama Pelanggan

Saldo

Rp.

☐

Foto

Verifikasi PIN

Kesempatan Verifikasi PIN 8 kali

Penjualan

Pembelian

Isi Ulang

Personalisasi

No. Transaksi

Tanggal Transaksi

Jumlah Setoran

☐

Untuk melakukan pengisian ulang, dapat memilih sistem paket atau non paket

☐ Paket

☐ Non Paket

Jumlah Nominal

Rp.

v

Jumlah Nominal

Rp.

Terbilang :

Proses

Logout

PIN

Tutup

Masukkan Smart Card

Gambar 4.14 Rancangan antarmuka halaman isi ulang saldo pelanggan.

BAB V

IMPLEMENTASI PERANGKAT LUNAK

5.1 Batasan Implementasi.

Batasan dari implementasi sistem informasi transaksi prabayar dengan media *smart card* ini adalah sebagai berikut :

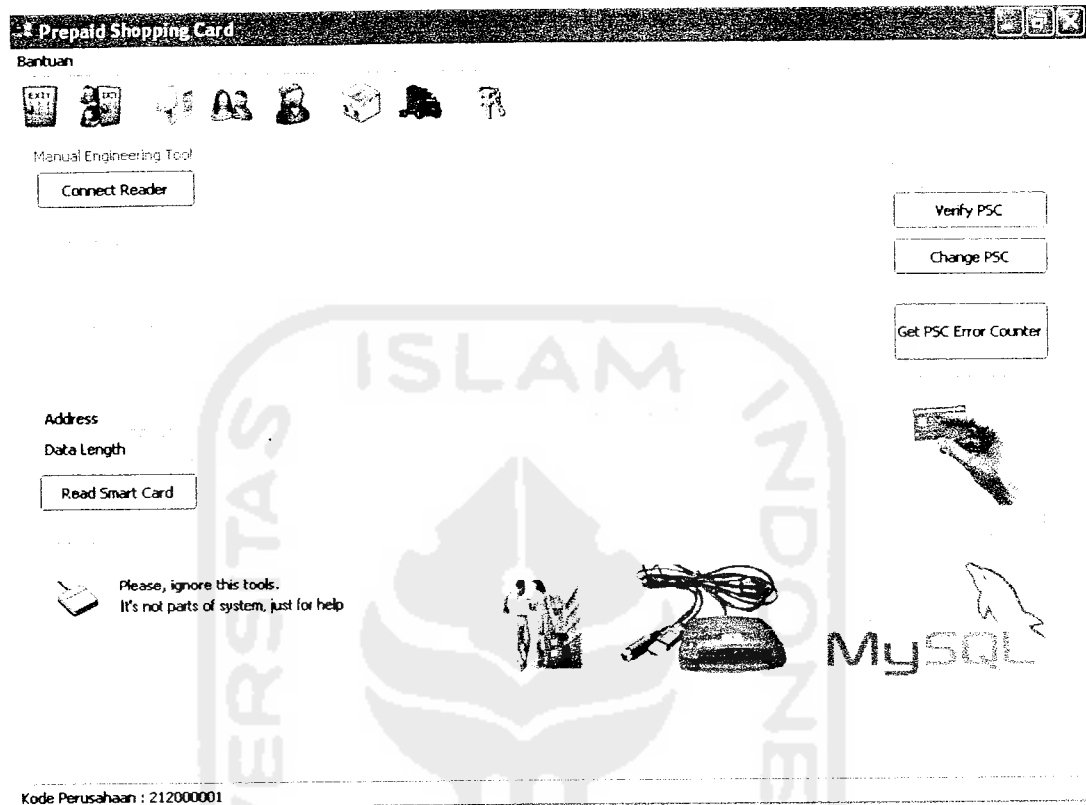
1. Sistem informasi transaksi prabayar ini dirancang sebagai simulasi sistem prabayar yang menitikberatkan pada pengimplementasian *smart card*.
2. Sistem ini dapat menangani personalisasi pelanggan, yang meliputi pengaturan pelanggan dan personalisasi kartu pelanggan.
3. Sistem ini dapat menangani pengaturan operator, pengaturan supplier, pengaturan barang.
4. Sistem ini dapat menangani pengolahan data transaksi pembelian, penjualan, pengisian ulang saldo kartu pelanggan.
5. Sistem ini menggunakan algoritma DES dan random key generator untuk keamanan data. Proses enkripsi dan dekripsi dengan algoritma DES akan menggunakan fungsi yang sudah disiapkan oleh pembuat *smart card reader* sebagai *software development kit* dalam bentuk file DLL.

6. Sistem ini dirancang untuk perusahaan bertipe usaha dagang secara retail yang mengasumsikan harga beli barang sama dengan harga jual barang.
7. Proses pengaturan pelanggan terdiri dari penambahan, pengubahan, penghapusan dan melihat data pelanggan. Proses ini hanya dapat dilakukan pada saat pelanggan memberikan *smart card*-nya untuk melakukan proses-proses tersebut.

5.2 Implementasi Perangkat Lunak

5.2.1 Halaman Utama Sistem Informasi Transaksi Prabayar.

Untuk dapat menjadi *client* dari sistem informasi transaksi prabayar ini, pertama kali perusahaan harus melakukan registrasi terlebih dahulu pada sistem *server* yang menyertakan data perusahaan dan data administrator. Data perusahaan meliputi : Nama perusahaan, Alamat perusahaan, Telepon perusahaan, Nama pemilik, alamat email perusahaan. Sedangkan data administrator meliputi : Nama, alamat, telepon, jenis kelamin, foto, alamat email. Setelah perusahaan berhasil melakukan registrasi pada *server* maka sistem siap diimplementasikan pada sisi *client*. Menu utama dari sistem ini dapat dilihat pada gambar 5.1.

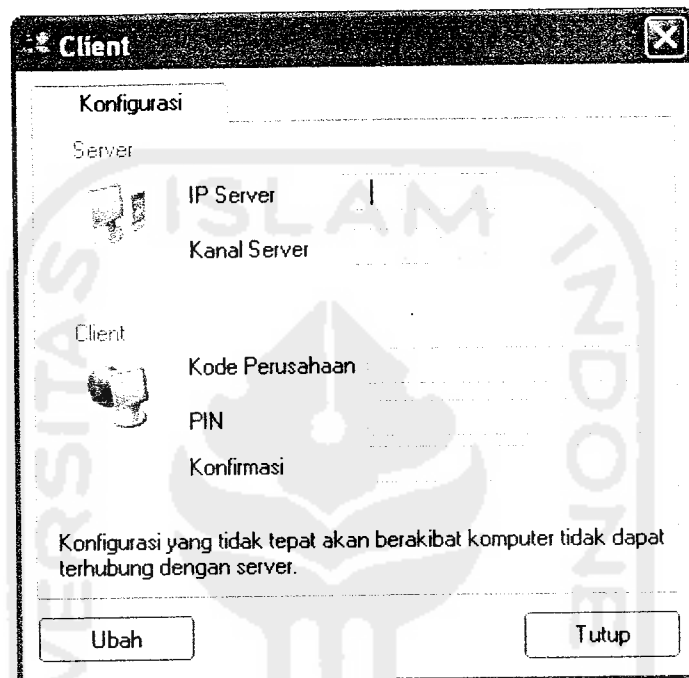


Gambar 5.1 Halaman Utama Sistem Informasi Transaksi Prabayar

5.2.2 Halaman Konfigurasi Jaringan.

Setelah server menerima data perusahaan dan data administrator dari perusahaan yang melakukan registrasi maka perusahaan akan mendapatkan data-data sebagai berikut : *IP address server*, nomor *port server*, nama *database server*, kode perusahaan, kunci publik atau kunci umum, kode administrator, dan PIN administrator. *IP address server*, nomor *port server*, nama *database server* dan kode perusahaan berguna untuk mengatur konfigurasi jaringan saat perusahaan pertama kali menjalankan sistem

informasi transaksi prabayar tersebut. Halaman konfigurasi jaringan dapat dilihat pada gambar 5.2



Client

Konfigurasi

Server

IP Server

Kanal Server

Client

Kode Perusahaan

PIN

Konfirmasi

Konfigurasi yang tidak tepat akan berakibat komputer tidak dapat terhubung dengan server.

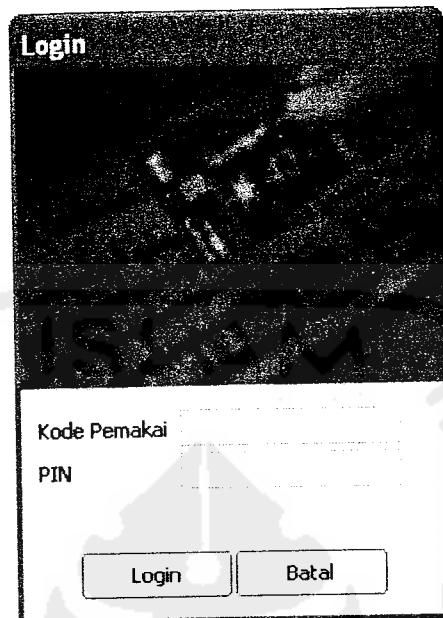
Ubah

Tutup

Gambar 5.2 Halaman Konfiguasi Jaringan

5.2.3 Halaman Login.

Pada saat sistem akan dioperasikan, maka sistem akan meminta pemakai atau pengguna dari sistem ini untuk login dengan memberikan kode pemakai beserta PIN. Halaman login dapat dilihat pada gambar 5.3.



Login

Kode Pemakai

PIN

Login Batal

Gambar 5.3 Halaman Login

5.2.4 Halaman Pengaturan Operator.

Halaman pengaturan operator ini adalah hak akses dari administrator, yang berguna untuk melakukan penambahan, pengubahan, penghapusan dan melihat data operator dari suatu perusahaan.

Halaman ini ditujukan bagi administrator untuk mendaftarkan operator yang akan bertugas sesuai dengan hak akses yang diberikan. Hak akses dibagi menjadi 5 bagian yaitu:

1. Pembelian, bertugas untuk melayani transaksi pembelian barang oleh perusahaan dari supplier.
2. Penjualan, bertugas untuk melayani transaksi penjualan barang kepada pelanggan menggunakan *smart card* secara prabayar.

3. Penambahan saldo, bertugas untuk melayani proses penambahan uang pelanggan pada *smart card*.
4. Personalisasi pelanggan, bertugas untuk melayani proses personalisasi pelanggan yang terdiri dari pengaturan pelanggan dan personalisasi kartu pelanggan.
5. Pengaturan barang, bertugas untuk melayani proses pengolahan data barang, yaitu : penambahan, pengubahan, penghapusan dan melihat data barang.

Pengaturan Operator

Operator

Kode Operator : 103002001

Nama

Alamat

Kota

Telepon

E-Mail

Jenis Kelamin

Nilai Baku

Hak Akses

Konfirmasi

Kode	Nama	Status
------	------	--------

Tambah Ubah Hapus Tutup

Gambar 5.4 Halaman Pengaturan Operator

5.2.5 Halaman Pengaturan Barang

Halaman pengaturan barang ini berguna untuk menangani proses memasukkan, pengubahan, penghapusan dan melihat data barang. Halaman ini dioperasikan oleh operator yang memiliki hak akses untuk menangani pengaturan barang.

Pengaturan Barang

Barang

Data

Kode Barang

Nama Barang

Harga

Kode Barang	Nama Barang	Harga Satuan (Rp)	Stok
-------------	-------------	-------------------	------

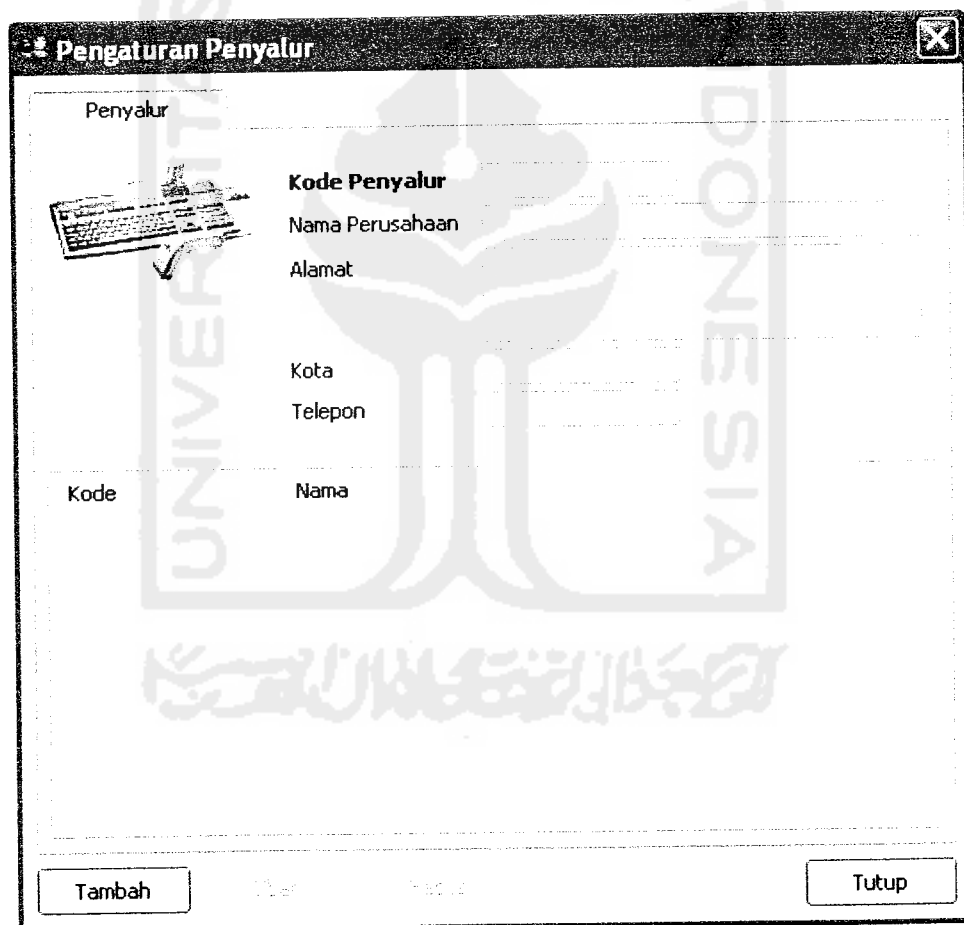
Total Barang: 0 item.

Tambah Ubah Hapus Tutup

Gambar 5.5 Halaman Pengaturan Barang

5.2.6 Halaman Pengaturan Suplier.

Halaman pengaturan suplier ini berguna untuk menangani proses memasukkan, pengubahan, penghapusan dan melihat data suplier. Halaman ini dioperasikan oleh operator yang memiliki hak akses untuk menangani pengaturan suplier.



Pengaturan Penyalur

Penyalur



Kode Penyalur

Nama Perusahaan

Alamat

Kota

Telepon

Kode	Nama
------	------

Tambah Ubar Hapus Tutup

Gambar 5.6 Halaman Pengaturan Suplier

5.2.7 Halaman Personalisasi Pelanggan.

Halaman personalisasi pelanggan ini berguna untuk menangani proses pengaturan pelanggan dan personalisasi kartu (*smart card*) pelanggan. Halaman ini dioperasikan oleh operator yang memiliki hak akses dalam proses personalisasi pelanggan.

Layanan Pelanggan

Informasi Kartu

Kode Pelanggan

Nama Pelanggan

Saldo Rp

Verifikasi PIN

Kesempatan verifikasi PIN 8 kali.

Not Available

Penjualan Pembelian Isi Ulang **Personalisasi**

Tanggal Registrasi :

Database

Jenis Kelamin

Alamat Tinggal

Kota

Telepon

Pekerjaan

Surat Elektronik

Nilai Baku

Status Aktif Non Aktif

P. I. N.

Konfirmasi

Tambah Ubah Hapus

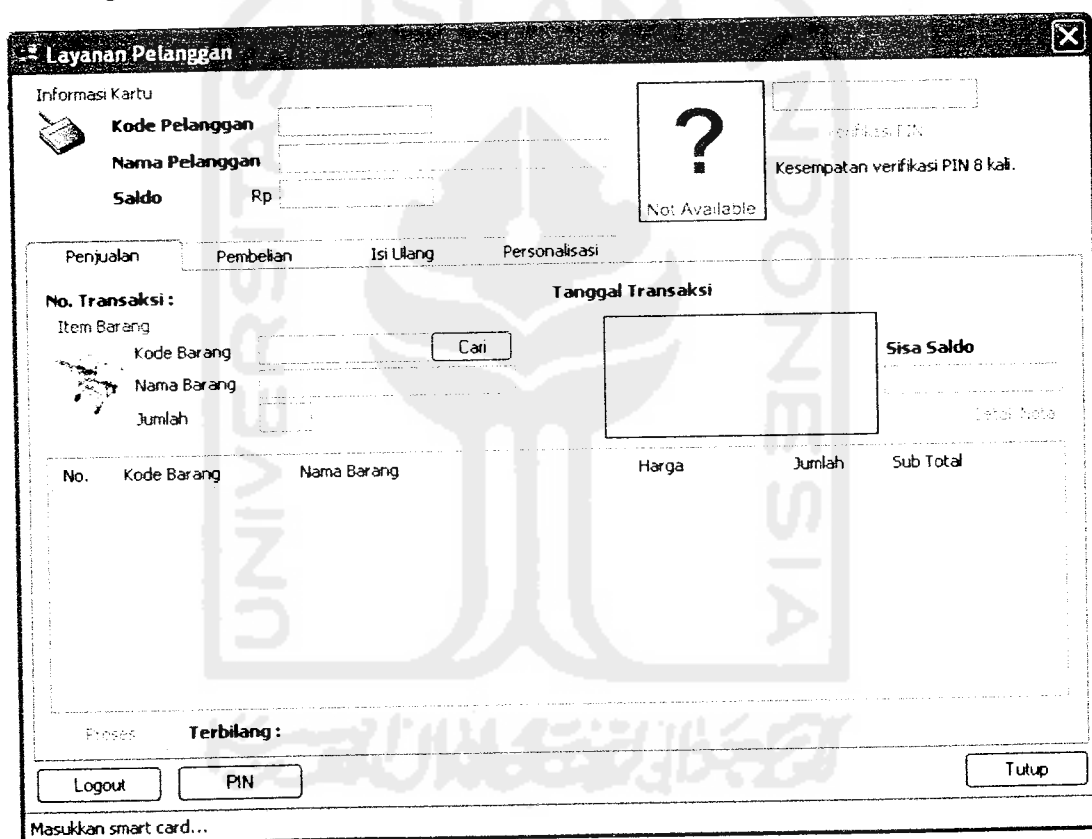
Logout PIN Tutup

Masukkan smart card...

Gambar 5.7 Halaman Personalisasi Pelanggan.

5.2.8 Halaman Penjualan.

Halaman penjualan ini berguna untuk menangani proses penjualan barang kepada pelanggan secara prabayar dengan menggunakan *smart card*. Halaman ini dioperasikan oleh operator yang memiliki hak akses dalam menangani proses penjualan.



Layanan Pelanggan

Informasi Kartu

Kode Pelanggan

Nama Pelanggan

Saldo Rp

Verifikasi PIN

Not Available

Kesempatan verifikasi PIN 8 kali.

Penjualan | Pembelian | Isi Ulang | Personalisasi

No. Transaksi :

Tanggal Transaksi

Item Barang

Kode Barang

Nama Barang

Jumlah

Sisa Saldo

Debit Note

No.	Kode Barang	Nama Barang	Harga	Jumlah	Sub Total

Proses Terbilang :

Masukkan smart card...

Gambar 5.8 Halaman Penjualan.

5.2.9 Halaman Pembelian.

Halaman pembelian ini berguna untuk menangani proses pembelian barang oleh perusahaan dari supplier. Sehingga dengan halaman ini perusahaan dapat menambahkan stok barang yang sudah ada. Halaman ini

Layanan Pelanggan

Informasi Kartu

 **Kode Pelanggan**

Nama Pelanggan

Saldo Rp

?
Not Available

Verifikasi PIN
Kesempatan verifikasi PIN 8 kali.

Penjualan Pembelian **Isi Ulang** Personalisasi

No. Transaksi : **Tanggal Transaksi**

Jumlah Setoran

 Untuk melakukan pengisian ulang, dapat memilih sistem paket atau non paket.

☒ Paket ☐ Non Paket

Jumlah Nominal Rp.

Jumlah Nominal Rp.

Terbilang : DUA RATUS LIMA PULUH RIBU RUPIAH

Masukkan smart card...

Gambar 5.10 Halaman Isi Ulang.

BAB VI

ANALISIS KINERJA PERANGKAT LUNAK

Setelah tahap implementasi perangkat lunak, tahap berikutnya adalah pengujian perangkat lunak. Pada tahap ini perangkat lunak akan diuji apakah masih ditemukan kesalahan-kesalahan pada perangkat lunak yang dibuat, selain itu juga membandingkan kebenaran dan kesesuaian dengan kebutuhan perangkat lunak. Pengujian perangkat lunak perlu dilakukan sebelum perangkat lunak tersebut diterapkan ke dalam lingkungan yang sebenarnya.

Pengujian data normal memiliki arti bahwa di dalam pengujian ini akan dilakukan sesuai dengan data sesungguhnya, yaitu dengan memperhatikan tipe data, panjang karakter, maupun kesesuaian data dengan sumber data. Sebagai contoh pada bab ini adalah pengujian masukan data, keluaran data.

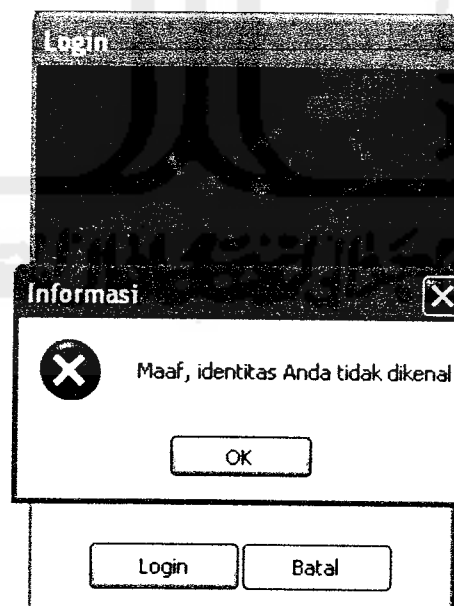
6.1 Pengujian Data Masukan

Pengujian dilakukan pada saat melakukan konfigurasi jaringan data yang dimasukkan tidak sesuai dengan konfigurasi yang dibutuhkan sistem. Pesan kesalahan akan dikirimkan dan terlihat seperti pada gambar 6.1. sedangkan pada gambar 6.2 merupakan kiriman pesan apabila saat pemakai

sistem melakukan login dimana data yang dimasukkan tidak sesuai dengan identitas login yang seharusnya.



Gambar 6.1 Pengujian Pemasukkan Data Konfigurasi Jaringan

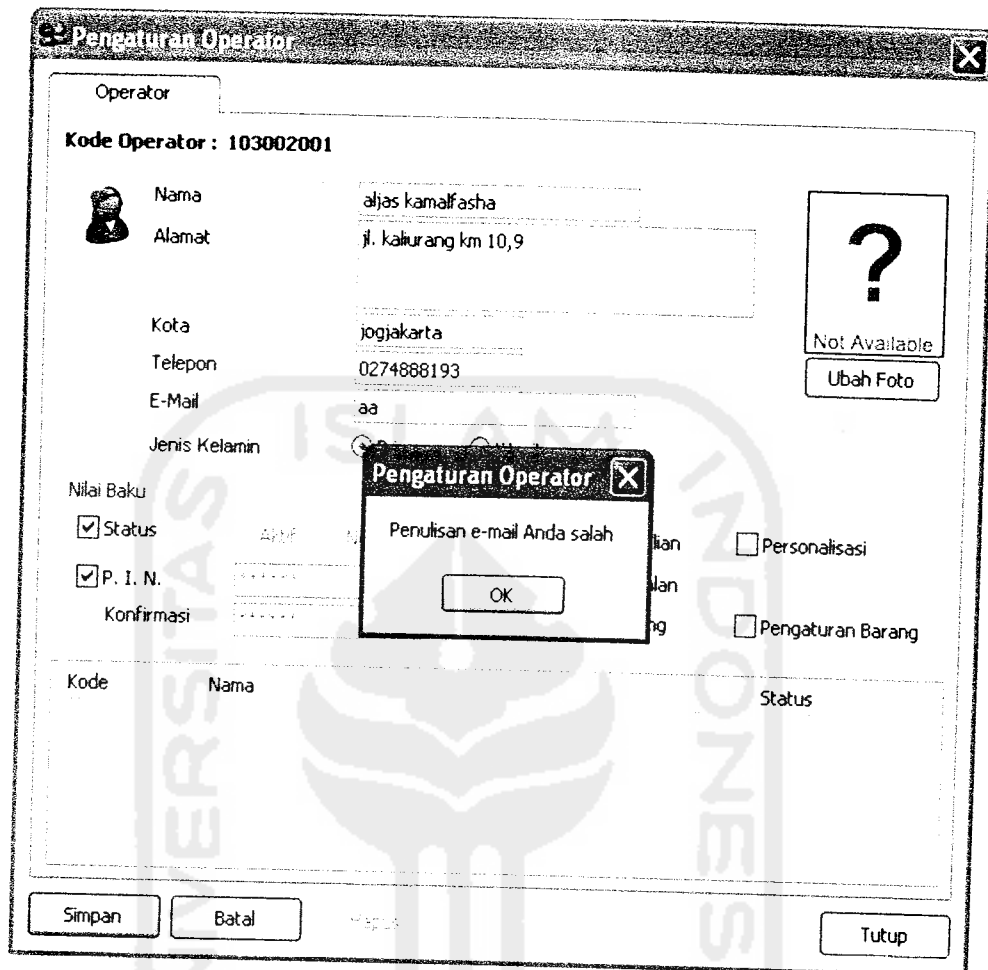


Gambar 6.2 Pengujian Pemasukkan Data Login Pemakai Sistem

Pengujian data masukkan dalam hal ini akan diberikan contoh memasukkan data operator melalui halaman pengaturan operator. Maka proses tidak dapat dilakukan sampai data operator yang dimasukkan sesuai dengan kebutuhan sistem, seperti ditunjukkan pada gambar 6.3, gambar 6.4

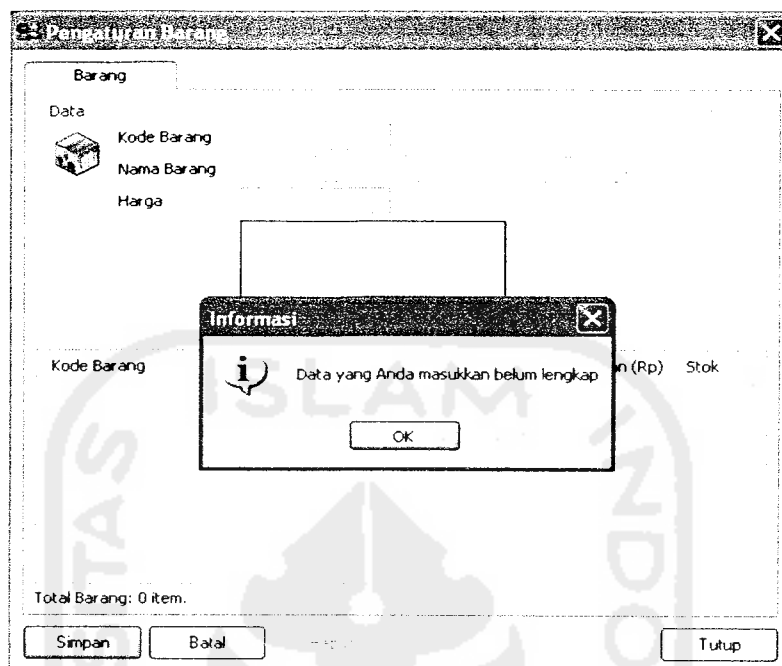
The screenshot shows a web application window titled "Pengaturan Operator". Inside, there's a form for adding a new operator. The form has fields for "Nama" (Name), "Alamat" (Address), "Kota" (City), "Telepon" (Telephone), "E-Mail", "Jenis Kelamin" (Gender), and "Nilai Baku" (Basic Value). A modal dialog box titled "Informasi" is overlaid on the form, displaying an information icon and the message "Data yang anda masukkan belum lengkap" (The data you entered is not complete), with an "OK" button. The background window also features a table with columns "Kode", "Nama", and "Status", and buttons "Tambah", "Ubah", "Hapus", and "Tutup".

Gambar 6.3 Pengujian Pemasukkan Data Operator yang tidak lengkap

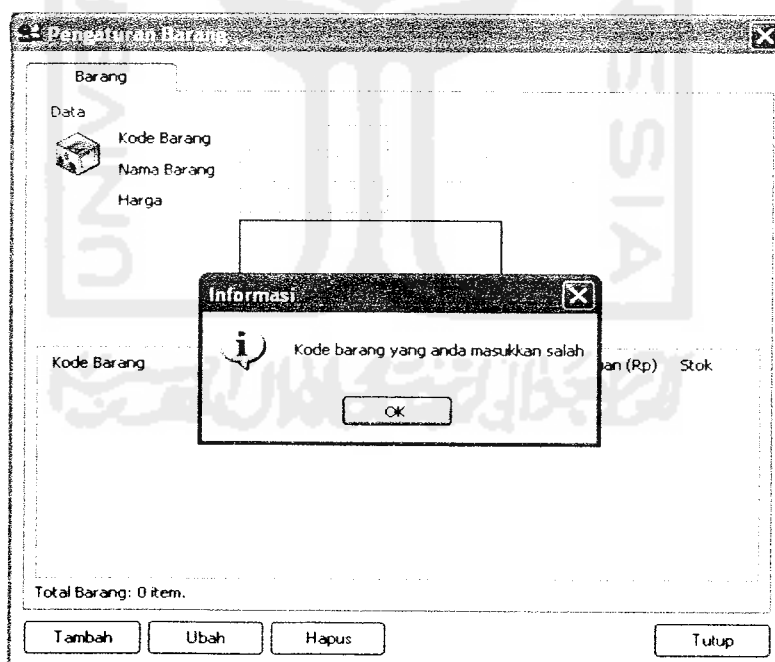


Gambar 6.4 Pengujian Pemasukkan alamat email Operator yang tidak sesuai dengan aturan sistem.

Pengujian data masukkan dalam memasukkan data barang melalui halaman pengaturan barang. Maka proses tidak dapat dilakukan sampai data barang yang dimasukkan sesuai dengan kebutuhan sistem, seperti ditunjukkan pada gambar 6.5, gambar 6.6.

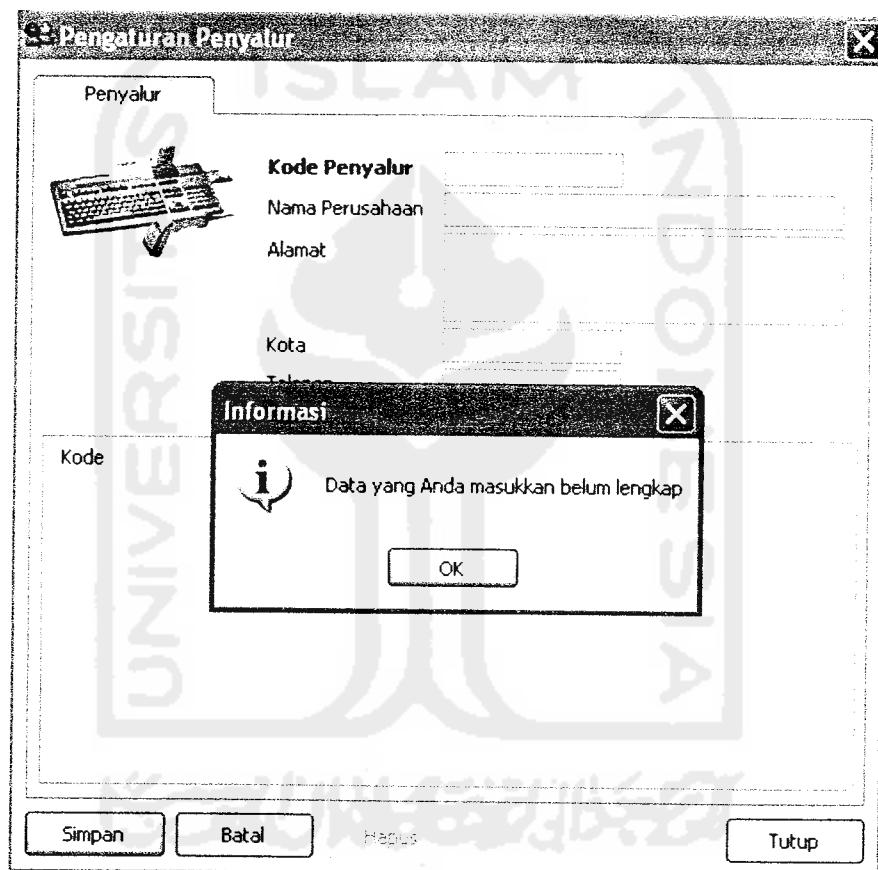


Gambar 6.5 Pengujian Pemasukkan Data Barang yang tidak lengkap



Gambar 6.6 Pengujian Pemasukkan Kode Barang yang tidak sesuai dengan aturan sistem

Pengujian data masukan dalam memasukkan data suplier melalui halaman pengaturan suplier. Maka proses tidak dapat dilakukan sampai data suplier yang dimasukkan sesuai dengan kebutuhan sistem, seperti ditunjukkan pada gambar 6.7.



Gambar 6.7 Pengujian Pemasukkan Data Suplier yang tidak lengkap

Pengujian pada saat *smart card* dimasukkan kedalam *smart card reader / writer*. Sistem akan mendeteksi apakah kartu *valid* atau tidak, apabila terjadi kesalahan maka sistem akan memberikan pesan didalam *status bar*

pada halaman personalisasi pelanggan, penjualan ataupun isi ulang saldo, seperti pada gambar 6.8

Layanan Pelanggan

Informasi Kartu

Kode Pelanggan

Nama Pelanggan

Saldo Rp

? Not Available

Kesempatan verifikasi PIN 8 kali.

Penjualan **Pembelian** **Isi Ulang** **Personalisasi**

No. Transaksi :

Item Barang

Kode Barang **Cari**

Nama Barang

Jumlah

Tanggal Transaksi

Sisa Saldo

No. **Kode Barang** **Nama Barang** **Harga** **Jumlah** **Sub Total**

Terbilang :

Logout **PIN** **Tutup**

Smart card tidak dapat dibaca.

Gambar 6.8 Pengujian Smart Card yang tidak dapat dibaca.

Pengujian pada saat pelanggan memasukkan PIN *smart card* yang tidak benar. Dalam sistem ini batas memasukkan PIN adalah sebanyak 8 kali. Hasil pengujian dapat dilihat pada gambar 6.9.

Layanan Pelanggan

Informasi Kartu

 **Kode Pelanggan** 002000001

Nama Pelanggan aljas kamalfasha

Saldo Rp 100000

 **Ubah Foto**

Verifikasi PIN

Kesempatan verifikasi PIN 8 kali.
PIN anda salah.
Sisa kesempatan 7 kali.

Penjualan Pembelian Isi Ulang Personalisasi

Tanggal Registrasi :

Database

 Jenis Kelamin ☒ Pria ☐ Wanita

Alamat Tinggal jl. kaliurang km 10,9

Kota jogjakarta

Telepon 0274888193

Pekerjaan direktur general contractor

Surat Elektronik aljas@auwoo.com

Nilai Baku

☐ Status ☒ Aktif ☐ Non Aktif

☒ P. I. N.

Konfirmasi

Simpan **Batal** **Hapus**

Logout **PIN** **Tutup**

Smart card aktif.

Gambar 6.9 Pengujian Pemasukkan PIN smart card yang tidak benar.

BAB VII

KESIMPULAN

7.1 Kesimpulan

Smart card dengan tipe SLE 4428, merupakan salah satu pilihan media dalam strategi bisnis pada sistem transaksi prabayar. Hal ini, *Smart card* dengan tipe SLE 4428 telah didukung oleh mekanisme perlindungan data dengan tambahan algoritma anti duplikasi, maka *smart card* dapat dijadikan media untuk tanda bukti transaksi dengan level sekuritas yang tergolong aman.

Adanya proses verifikasi 2 arah sangat membantu melindungi *smart card* dari tindakan mengubah data yang dilakukan secara sepihak baik oleh konsumen maupun penyedia jasa. Sebelum melakukan proses debit dan penambahan saldo maka akan dilakukan verifikasi berupa pemasukan PIN dari pihak konsumen. Tanpa adanya verifikasi dari konsumen maka jumlah saldo tidak dapat diubah oleh penyedia jasa. Demikian juga pihak penyedia jasa akan menggunakan PSC sebagai pengenal kartu yang akan diverifikasi oleh program aplikasi.

Dengan adanya verifikasi dari kedua belah pihak maka tidak akan terjadi kecurangan yang dapat mengakibatkan kerugian pada salah satu pihak.

Kerugian dalam sistem transaksi prabayar ini adalah uang pelanggan yang terdapat di dalam kartu atau *smart card* tidak bisa dicairkan kembali.

7.2 Saran

Simulasi ini menunjukkan bahwa *smart card* dapat dijadikan sebagai tanda bukti atau pengenalan dalam proses transaksi prabayar, sehingga untuk pengembangan lebih lanjut, penggunaan *smart card* dapat diimplementasikan pada media akses kontrol, kartu identitas dan lainnya.

Sistem informasi transaksi prabayar ini akan lebih optimal apabila sisi *client* memiliki *database* masing-masing didalam penyimpanan data, sehingga sistem *server* benar-benar hanya mengatur status masing-masing perusahaan dan mekanisme hutang piutang antara perusahaan – perusahaan *client*, dengan mempertimbangkan keamanan dan kecepatan akses data disarankan menggunakan *smart card* bertipe *contactless*.

DAFTAR PUSTAKA

- [BUD95] Budiharjo, E. *Sistem Informasi Manajemen*, diktata KPC
Pemrogramanan (bisnis), Bidang Pendidikan dan Pelatihan Pusat
Komputer PIKSI Institut Teknologi Bandung, 1995-1996
- [EVE99] Everett, B, David, Dr. *Smart Card Technology : Introduction to
Smart Card*, *Smart Card News Ltd* , 1999
- [GUT98] Guthery, Scott ; Jurgensen, Tim. *Smart Card Developer's Kit*,
Macmillan Computer Publishing, 1998
- [JOG99] Jogiyanto HM, *Analisis dan Desain Sistem Informasi Pendekatan
Terstruktur Teori dan Praktek Aplikasi Bisnis*, Yogyakarta: Andi
Offset, 1999
- [KRI03] Kristanto, Andri. *Keamanan Data Pada Jaringan Komputer*, Gava
Media, 2003.
- [McL98] McLeod, Raymond , jr. *Sistem Informasi Manajemen Jilid 1*, 1998
- [SIM95] Simatupang, T.M., *Teori Sistem: Suatu Perspektif Teknik Industri*,
Andi Offset, Jogjakarta, 1995
- [SUR98] Suryadi, K., Ramadhani, M.A., *Sistem Pendukung Keputusan*,
Remaja Rosdakarya, Bandung, 1998
- [VAN96] Van, Oorshot, P, Menezes, A, dan Vanstone, S. *Handbook of
Applied Cryptography*, CRC Press, 1996.

- [WAH02] Wahid, Fathul. *Kamus Istilah Teknologi Informasi*, Andi Offset, 2002
- [ACS02] Advanced Card System Ltd, *ACSR20 Smart Card Driver Program Reference Manual*, 2002
- [ACR02] Advanced Card System Ltd, *ACR30 Reference Manual*, 2002

