APLIKASI SECURE NOTES
DENGAN PUSTAKA BOUNCY CASTLE

TUGAS AKHIR

Oleh :

Andria Gutama **33105026**

Disusun untuk memenuhi syarat kelulusan Program Diploma III

PROGRAM STUDI TEKNIK INFORMATIKA
POLITEKNIK BATAM
BATAM

2008

LEMBAR PENGESAHAN
APLIKASI SECURE NOTES
DENGAN PUSTAKA BOUNCY CASTLE

Batam, Januari 2008

Pembimbing I	Pembimbing II
Metta Santiputri, M.Sc	**Rahmat Sagara, M.Si**
NIK. 100017	**NIK. 107046**

ABSTRAKSI

APLIKASI SECURE NOTES DENGAN PUSTAKA BOUNCY CASTLE

Andria Gutama, 33105026
(xi + 55)

Kebiasaan menyimpan catatan dan data pribadi yang bersifat rahasia di ponsel sudah tidak dapat dihindari. Catatan pribadi, catatan bisnis penting, nomor PIN kartu ATM/kartu kredit memang sudah seharusnya diletakkan di tempat yang mudah dijangkau dan selalu kita bawa ke mana-mana. Salah satunya adalah ponsel.

Menyimpan catatan dan data pribadi di ponsel tidak selalu aman. Oleh karena itu diperlukan suatu metode untuk memastikan bahwa catatn dan data pribadi yang kita simpan di ponsel dapat dijamin keamanannya.

Terkait hal tersebut, dikembangkanlah aplikasi Secure Notes dengan tujuan agar pemilik ponsel dapat menyimpan catatan dan data pribadi miliknya di dalam ponsel dengan aman.

Buku laporan yang berjudul “Aplikasi Secure Notes dengan Pustaka Bouncy Castle” ini berisi latar belakang dan tujuan pembuatan aplikasi Secure Notes, deskripsi umum aplikasi, analisis dan deskripsi perancangan aplikasi, serta hasil implementasi dan pengujian aplikasi Secure Notes.

Kata kunci : Data Pribadi, Password, RC4, MD5, Enkripsi, Dekripsi, Key.

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa atas berkah dan karunia-Nya sehingga penyusun dapat menyelesaikan Laporan Tugas Akhir yang berjudul "Aplikasi Secure Notes dengan Pustaka Bouncy Castle" ini.

Aplikasi Secure Notes ini dibuat dengan tujuan agar pemilik ponsel dapat menyimpan data pribadi di dalam ponsel miliknya dengan aman.

Dalam kesempatan ini, penyusun ingin menyampaikan ucapan terima kasih kepada :

1. Allah SWT atas karunia-Nya yang tidak terbatas,
2. Nabi Muhammad SAW sebagai teladan bagi umat manusia,
3. Kedua orangtua dan keluarga yang telah memberikan dukungan moral dan materi,
4. Buat seseorang yang selalu membantu dan mendukung penyusun. Atas sms-smsnya yang selalu bilang 'Kak, selesaikan dunk TA nya…',
5. Teman-teman dari Informatika angkatan 2005 atas dukungan dan kerjasamanya,
6. Teman-teman dari Informatika angkatan 2006 dan Informatika angkatan 2007 atas dukungannya,
7. Ibu Mettasanti Putri selaku koordinator Tugas Akhir sekaligus dosen pembimbing I,
8. Ibu Evaliata Sembiring selaku koordinator Tugas Akhir,
9. Bapak Rahmat Sagara selaku dosen pembimbing II,
10. Bapak Andy Triwinarko atas perdebatannya yang panjang tentang enkripsi, dekripsi dan kunci,
11. Seluruh dosen Teknik Informatika yang telah memberikan arahan melalui saran dan kritiknya,
12. Serta pihak-pihak lain yang turut membantu dalam penyelesaian Tugas Akhir,

Penyusun menyadari bahwa masih terdapat kekurangan dalam penyusunan buku Laporan Tugas Akhir ini. Untuk itu, penyusun mengharapkan kritik dan saran yang konstruktif dari pembaca sehingga dapat dicapai suatu kesempurnaan.

Semoga buku ini dapat bermanfaat bagi pembaca, khususnya bagi yang hendak mengembangkan aplikasi serupa.

Batam, 22 Januari 2008

Penyusun

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISI LAMPIRAN

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Kebiasaan menyimpan catatan dan data pribadi yang bersifat rahasia di ponsel sudah tidak dapat dihindari. Catatan pribadi, catatan bisnis penting, nomor PIN kartu ATM/kartu kredit memang sudah seharusnya diletakkan di tempat yang mudah dijangkau dan selalu kita bawa ke mana-mana. Salah satunya adalah ponsel.

Menyimpan data pribadi di ponsel tidak selalu aman. Bisa saja ponsel anda hilang atau ada orang lain yang melihat isi ponsel anda tanpa seizin anda. Jika tidak hati-hati, rahasia pribadi anda bisa disalahgunakan oleh orang yang tidak bertanggungjawab.

Dengan adanya aplikasi Secure Notes ini, setiap pemilik ponsel dapat menyimpan data pribadi miliknya secara persisten dengan aman. Aplikasi Secure Notes ini akan mengenkripsi setiap data di dalamnya memastikan data benar-benar aman. Selain itu, aplikasi dilindungi dengan *password*.

Aplikasi Secure Notes menggunakan pustaka Bouncy Castle untuk enkripsi data. Bouncy Castle adalah salah satu pustaka enkripsi yang tersedia secara *free* dan *open source* untuk platform Java.

1.2 Tujuan

Dengan adanya aplikasi ini diharapkan mampu:

- Menyimpan data pribadi dan rahasia di ponsel secara persisten dengan aman

1.3 Batasan Masalah

Batasan masalah aplikasi Secure Notes adalah sebagai berikut:

- Data yang disimpan hanya berupa teks

1.4 Ikhtisar Buku

Sistematika penulisan laporan ini adalah sebagai berikut:

Bab I Pendahuluan, membahas latar belakang dan tujuan pembuatan aplikasi, Batasan Masalah dan Ikhtisar Buku. Sub bab Latar Belakang menjelaskan alasan mengapa aplikasi ini perlu dirancang. Sub bab Batasan Masalah menjelaskan hal-hal yang menjadi batasan aplikasi.

Bab II Deskripsi Umum Sistem, memaparkan sistem aplikasi secara umum, karakteristik pengguna, lingkungan operasi aplikasi, dan aturan penamaan. Sub bab Deskripsi Umum Sistem menjelaskan spesifikasi dan kegunaan aplikasi. Sub bab Karakteristik Pengguna berisi informasi mengenai pengguna aplikasi. Sub bab Lingkungan Operasional berisi informasi mengenai lingkungan operasional aplikasi. Sub bab Aturan Penamaan menjelaskan aturan penamaan yang digunakan dalam aplikasi ini.

Bab III Analisis, berisi deskripsi perangkat keras, hubungan antara perangkat keras dengan perangkat lunak, dan deskripsi fungsional. Sub bab Deskripsi Perangkat Keras memaparkan tentang deskripsi perangkat keras yang digunakan dalam aplikasi. Pada sub bab Hubungan Antara Perangkat Keras dan Perangkat Lunak menjelaskan hubungan antara perangkat keras yang digunakan dengan aplikasi. Sub bab Deskripsi Fungsional berisi context diagram dan diagram alir data (DFD) dari aplikasi.

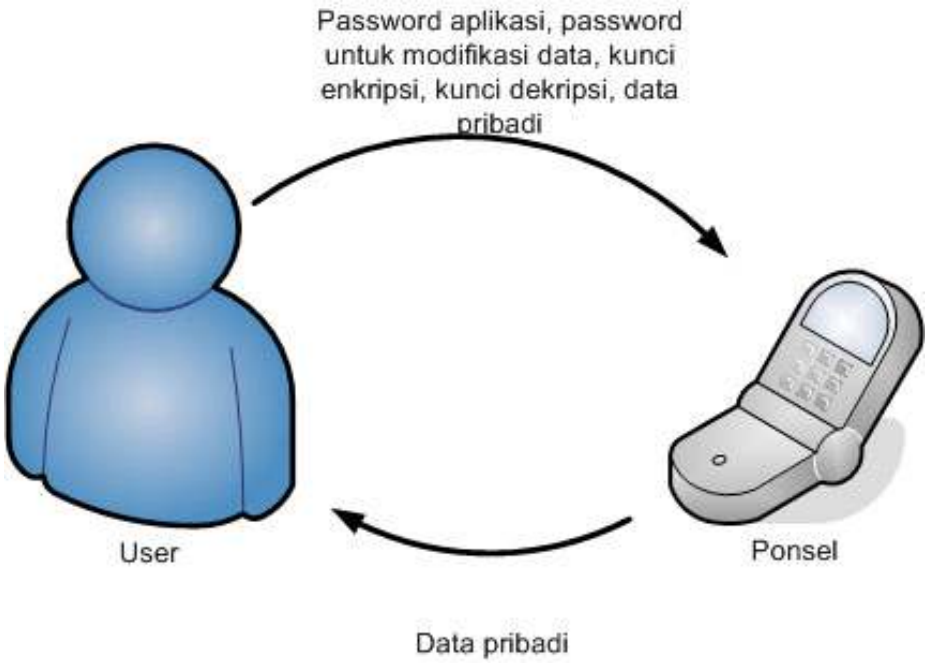
Bab IV Deskripsi Perancangan, membahas deskripsi data, dekomposisi fungsional modul, spesifikasi kebergantungan antar layar, dan struktur menu. Sub bab Deskripsi Data berisi deskripsi data yang dikelola dalam aplikasi. Sub bab Dekomposisi Fungsional Modul menjelaskan daftar input-proses-output aplikasi Secure Notes. Sub bab Spesifikasi Kebergantungan Antar Layar menjelaskan kebergantungan antar layar dalam aplikasi ini. Sub bab Struktur Menu menggambarkan struktur menu aplikasi Secure Notes.

Bab V Implementasi dan Pengujian, berisi pustaka yang digunakan, spesifikasi kebergantungan antar modul, struktur direktori dan deskripsi file, serta pengujian dan hasilnya. Sub bab Pustaka yang digunakan menjelaskan tentang pustaka yang digunakan dalam aplikasi ini. Sub bab Spesifikasi Kebergantungan Antar Modul menggambarkan kebergantungan antar modul dalam aplikasi ini. Sub bab Struktur Direktori dan Deskripsi File berisi daftar direktori dan file aplikasi Secure Notes. Sub bab Pengujian dan Hasil berisi tentang pengujian terhadap fungsi-fungsi dalam pembuatan aplikasi serta hasil pengujiannya.

Bab VI Kesimpulan dan Saran, memuat kesimpulan dari perancangan aplikasi dan saran untuk pengembangan lebih lanjut aplikasi Secure Notes ini.

BAB 2 DESKRIPSI UMUM APLIKASI

2.1 Deskripsi Umum Sistem



Gambar 2-1 Deskripsi Umum Sistem Aplikasi Secure Notes

User akan memasukkan *password* untuk menggunakan aplikasi ini. Aplikasi akan memeriksa *password* tersebut dan bila benar, user boleh menggunakan aplikasi ini. Selanjutnya user dapat melihat, menambah, merubah, ataupun menghapus data pibadinya yang telah ada dalam aplikasi dalam kategori tertentu. User diharuskan untuk memasukkan kunci enkripsi setiap kali ingin menambah data pribadi dan kunci dekripsi setiap kali ingin melihat kembali data pribadi yang telah ada. Setiap data pribadi terdiri atas judul data, kategori data pribadi, waktu pembuatan data, dan detail data pribadi. Setiap data pribadi yang dimasukkan oleh user akan dienkripsi oleh aplikasi.

2.2 Karakteristik Pengguna

Tabel 2-1 Kategori Pengguna Aplikasi

Kategori Pengguna	Tugas	Hak Akses ke Aplikasi	Jabatan
User terotentikasi	Menyimpan data pribadi dan rahasia ke dalam aplikasi	Hak akses penuh terhadap semua fasilitas aplikasi	User

2.3 Batasan

- Aplikasi Secure Notes menggunakan pustaka kriptografi Bouncy Castle
- Algoritma kriptografi yang dipakai untuk enkripsi data pribadi adalah RC4
- Algoritma kriptografi yang dipakai untuk enkripsi kunci enkripsi dan kunci dekripsi adalah MD5
- Algoritma kriptografi yang dipakai untuk enkripsi password aplikasi adalah MD5

2.4 Lingkungan Operasional

Aplikasi Secure Notes mempunyai dua lingkungan operasional yaitu perangkat keras dan perangkat lunak yaitu:

2.4.1 Perangkat Keras

Spesifikasi perangkat keras ponsel yang bisa menggunakan aplikasi ini adalah sebagai berikut:

a. Configuration : Connected Limited Device Configuration (CLDC) 1.1
b. Profile : Mobile Information Device Profile (MIDP) 2.0

2.4.2 Perangkat Lunak

Spesifikasi perangkat lunak ponsel yang bisa menggunakan aplikasi ini adalah sebagai berikut:

a. Sistem Operasi : Java / Symbian 2.0
b. Program/ Utilitas lain : Pustaka Bouncy Castle

2.5 Aturan Penamaan

Penamaan dalam aplikasi ini menggunakan aturan sebagai berikut:

a. Class diberi nama sesuai dengan kegunaannya.
   Misal Class sebagai deskprisi data pribadi dinamai Class DataPribadi.
b. Method diberi nama sesuai dengan perilakunya.
   Misal Method untuk penggunaan enkripsi data pribadi dinamai EnkripsiDataPribadi.
c. Form diberi nama sesuai dengan isi layarnya.
   Misal form layar login diberi nama FormLayarLogin.

BAB 3 ANALISIS

3.1 Deskripsi Perangkat Keras

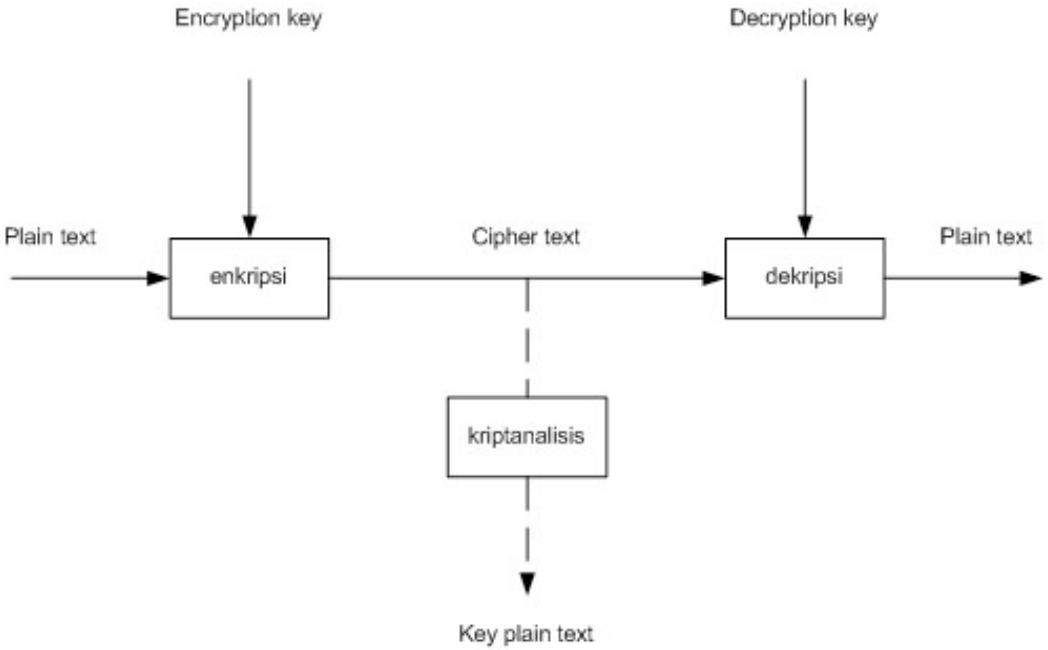
Gambar 3.1 Ponsel

Perangkat keras yang digunakan dalam aplikasi Secure Notes adalah ponsel dengan merk Nokia seri 3310 Classic, Nokia N70, dan Sony Ericsson W880i.
Ponsel lain yang bisa diimplementasikan oleh aplikasi Secure Notes adalah ponsel yang mendukung platform Java MIDP 2.0.

3.2 Hubungan Antara Perangkat Keras dengan Perangkat Lunak

Aplikasi Secure Notes adalah aplikasi yang diimplementasikan kepada ponsel yang mendukung platform Java MIDP 2.0. Untuk mengirim aplikasi Secure Notes dari komputer ke ponsel dapat menggunakan kabel data yang didukung oleh ponsel tersebut.

Sistem Kriptografi :



Gambar 3.2 Sistem Kriptografi

Kriptografi adalah ilmu yang berguna untuk mengacak data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga. Data yang diacak harus bisa dibaca kembali oleh pihak yang berwenang.
Data yang ingin diacak disebut *plain text*. Data diacak dengan menggunakan kunci enkripsi *(encryption key)*. Proses pengacakan itu sendiri disebut enkripsi (*encryption*). *Plain text* yang telah diacak disebut *cipher text*. Proses untuk mengembalikan *cipher text* menjadi *plain text* disebut dekripsi (*decryption*). Kunci yang digunakan pada tahap dekripsi disebut kunci dekripsi (*decryption key*).
Pada prakteknya, selain pihak yang berwenang terhadap data yang diacak tersebut, ada juga pihak ketiga yang selalu berusaha untuk mengembalikan *cipher text* ke *plain text* atau memecahkan kunci dekripsi. Usaha oleh pihak ketiga ini disebut kriptanalisis (*cryptanalysis*).

Proses kriptografi adalah proses yang sangat rumit dan cukup menyita sumber daya. Hal tersebut tentu saja tidak cocok diimplementasikan pada ponsel yang terikat oleh sumber daya baterainya. Oleh karena itu, diperlukan suatu proses kriptografi yang cukup ampuh tetapi tidak terlalu menyita banyak sumber daya.

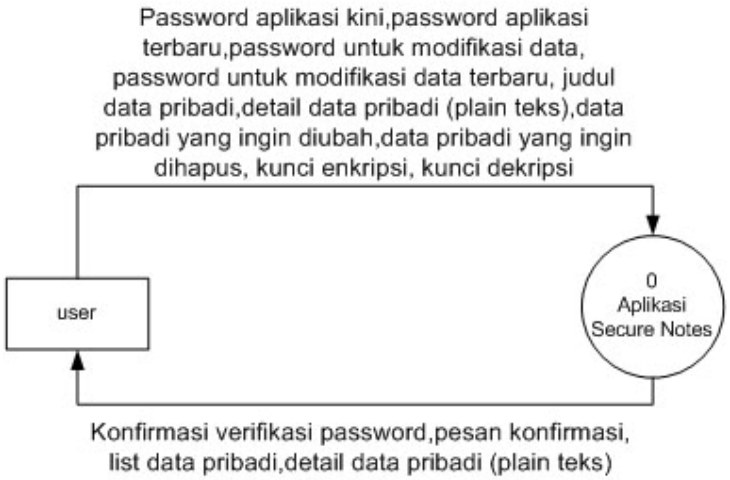
Pustaka Bouncy Castle adalah salah satu pustaka kriptografi yang bisa diimplementasikan pada ponsel karena selain memiliki kemampuan yang cukup baik, ia tidak banyak menyita sumber daya ponsel.

Beberapa metode kriptografi yang didukung oleh pustaka kriptografi Bouncy Castle antara lain : RSA, DES, AES (Rijndael), Blowfish, CAST, ElGamal, Twofish, IDEA, RC2, RC4, MD2, MD4, MD5, GOST-34.11, RIPEMD128, RIPEMD160, RIPEMD256, RIPEMD320, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, Tiger, Whirlpool, X.509v3 dan sebagainya.

3.3 Deskripsi Fungsional

Deskripsi Fungsional menjelaskan context diagram aplikasi Secure Notes beserta diagram alir datanya.

3.3.1 Context Diagram



Gambar 3.3 Context Diagram Aplikasi Secure Notes

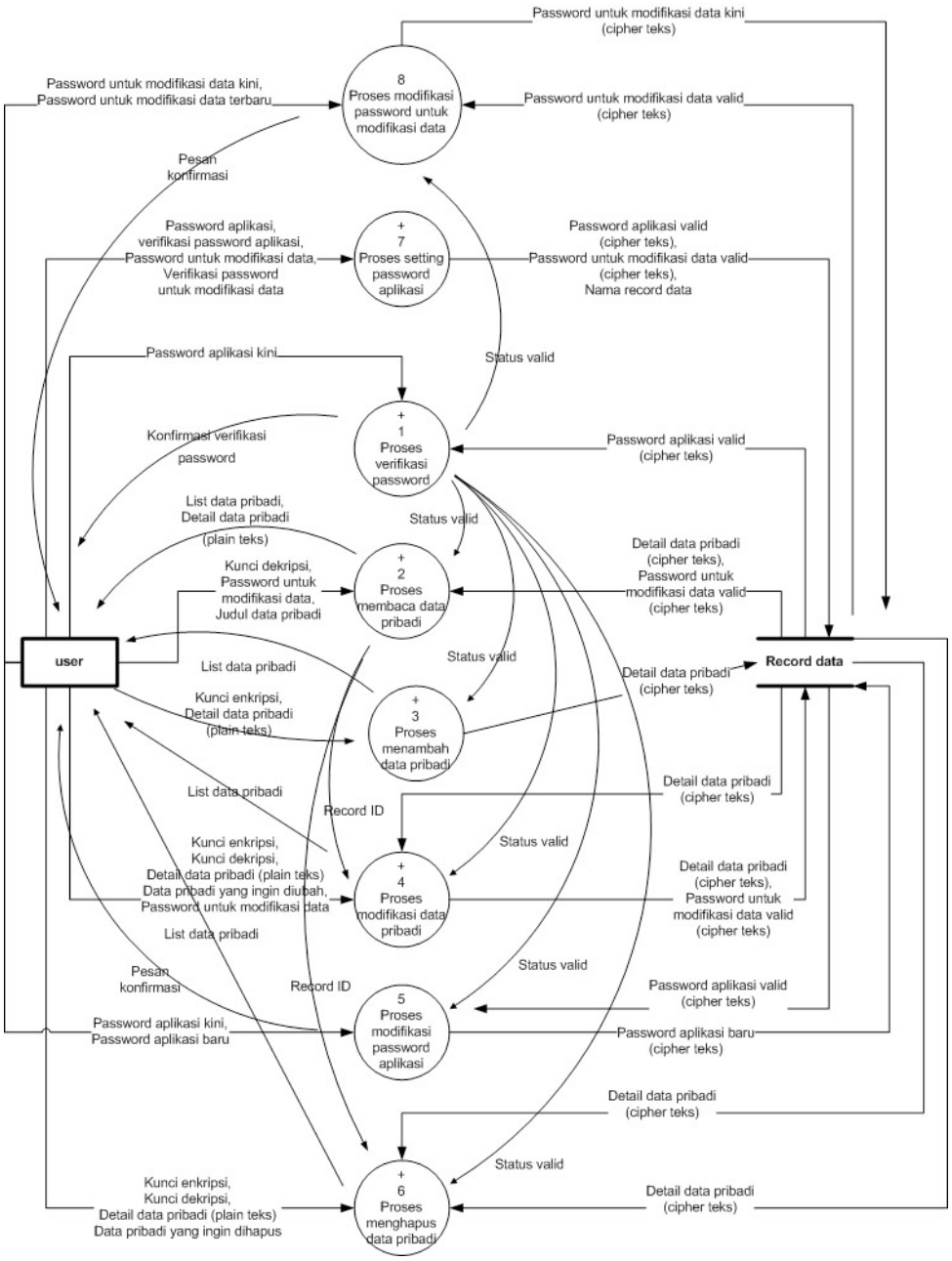
User akan memasukkan *password* untuk menggunakan aplikasi ini. Data *password* aplikasi akan dienkripsi dengan algoritma kriptografi MD5. Aplikasi akan memeriksa *password* tersebut dan bila benar, *user* boleh menggunakan aplikasi ini. Selanjutnya *user* dapat melihat, menambah, merubah, ataupun menghapus data pibadinya yang telah ada dalam aplikasi. Setiap data pribadi terdiri atas judul data, waktu pembuatan data, kategori data dan detail data pribadi. Setiap data pribadi yang dimasukkan oleh *user* akan dienkripsi oleh aplikasi dengan algoritma kriptografi RC4.

Spesifikasi aplikasi Secure Notes :

- Aplikasi mampu menyimpan data pribadi pengguna dalam kategori tertentu ke dalam ponsel.
- Aplikasi mampu mengenkripsi data pribadi pengguna dengan metode enkripsi yang tersedia dalam pustaka Bouncy Castle. Algoritma kriptografi yang digunakan untuk enkripsi *password* aplikasi dan enkripsi kunci enkripsi/ kunci dekripsi adalah MD5, sedangkan algoritma kriptografi yang digunakan untuk enkripsi dan dekripsi data pribadi adalah RC4.
- Aplikasi mampu menambah, menghapus dan mengedit data pribadi sesuai keinginan pengguna.

3.3.2 DFD Level 1

DFD Level 1 menggambarkan semua proses umum yang terdapat dalam aplikasi Secure Notes.



Gambar 3.4 DFD Level 1 Aplikasi Secure Notes

Proses 1

Proses 1 Verifikasi Password menerima data input dari *user* berupa password aplikasi kini. Proses juga mengambil password aplikasi valid (*cipher text*). Terjadi proses pencocokan kedua data tersebut. Proses akan menghasilkan data kofirmasi verifikasi password dan data status valid jika *user* tersebut mempunyai hak untuk mengakses aplikasi. Data output berupa konfirmasi verifikasi password dan data valid.

Proses 2

Proses 2 Membaca Data Pribadi menerima data input berupa status valid dari proses sebelumnya, detail data pribadi (*cipher text*) dari record store. Detail data pribadi tersebut akan didekripsi. Proses akan menghasilkan record ID,list data pribadi dan detail data pribadi dalam bentuk *plain text*. Selanjutnya *user* dapat membaca data pribadi yang diinginkan dengan memilih judul data pribadi yang ada.

Proses 3

Proses 3 Menambah Data Pribadi menerima data input berupa status valid dari proses sebelumnya, dan detail data pribadi dalam bentuk *plain text*. Proses akan memvalidasi data tersebut, mengenkripsinya sehingga menghasilkan detail data pribadi dalam bentuk *cipher text*. Detail data pribadi (*cipher text*) tersebut selanjutnya disimpan ke dalam record store.

Proses 4

Proses 4 Modifikasi Data Pribadi. *User* memilih data pribadi yang ingin dimodifikasi. Selanjutnya proses akan membaca detail data pribadi (*cipher text*) dari record store dan mendekripsikannya sehingga menjadi detail data pribadi (*plain text*). Detail data pribadi (*plain text*) tersebut diberikan kepada *user*. Selanjutnya *user* dapat memodifikasi detail data pribadi tersebut. Detail data pribadi hasil modifikasi akan dienkripsi dan disimpan ke dalam record store.

Proses 5

Proses 5 Modifikasi Password Aplikasi menerima data input dari *user* berupa password aplikasi kini dan password aplikasi terbaru. Proses akan membaca password aplikasi valid (*cipher text*) dari record store. Terjadi proses pencocokan antara password aplikasi kini dengan password aplikasi valid. Jika ternyata cocok, proses akan menyimpan password aplikasi terbaru ke dalam record store. Datra output berupa pesan konfirmasi ke *user*.

Proses 6

Proses 6 Menghapus Data Pribadi menerima data input berupa detail data pribadi (*cipher text*) dari record store. Proses akan mendekripsikan detail data pribadi tersebut dan memberikan list data pribadi kepada *user*. Selanjutnya *user* memilih data pribadi mana yang ingin dihapus melalui list data pribadi tersebut. Selanjutnya proses akan memperbarui isi record store. Data output berupa list data pribadi yang disampaikan ke *user*.

Proses 7

Proses 7 Setting Password Aplikasi adalah proses yang dijalankan ketika aplikasi Secure Notes dijalankan untuk pertama kalinya. Proses ini Menerima input dari *user* berupa password aplikasi dan verifikasi password aplikasi. Proses akan menenkripsi password aplikasi dan menyimpan informasi password pada record store.

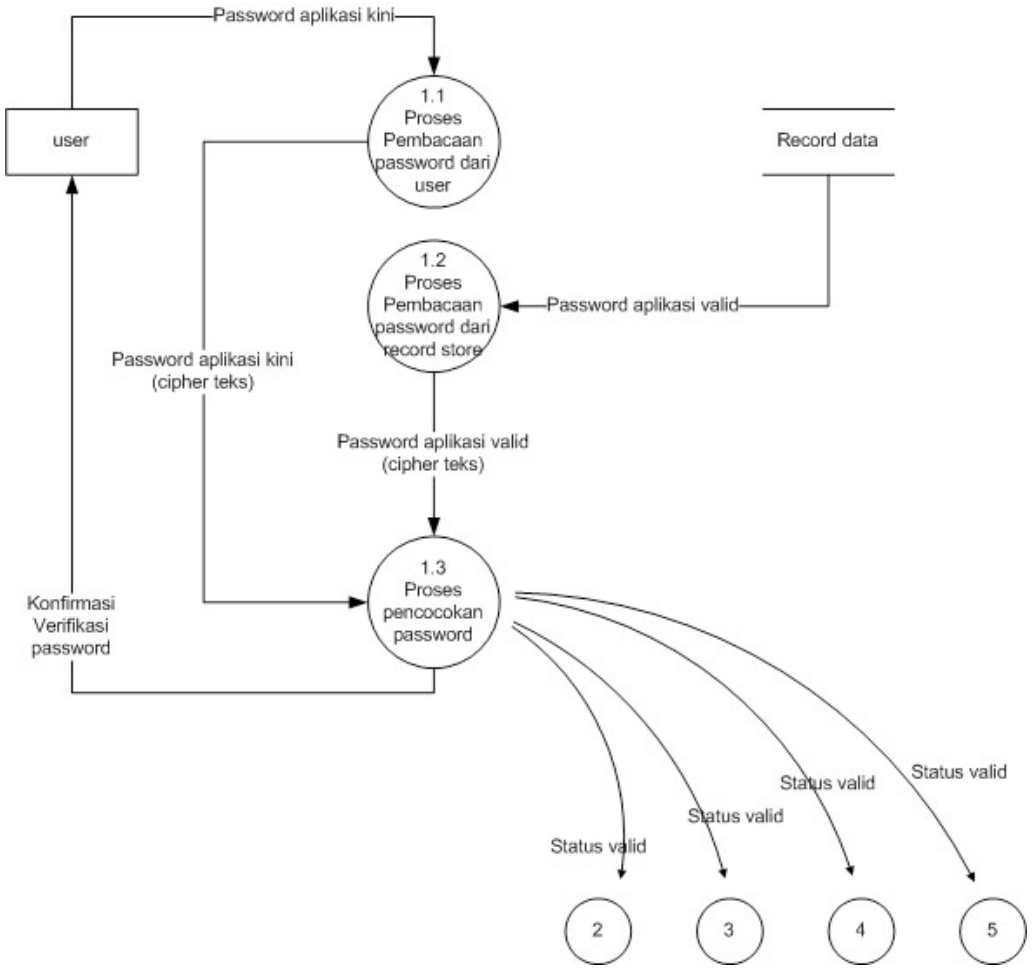
Proses 8

Proses 8 Modifikasi Password untuk Modifikasi Data adalah proses untuk merubah password untuk modifikasi data. Proses ini menerima input dari *user* berupa password untuk modifikasi data kini dan password untuk modifikasi data terbaru. Proses akan membaca password untuk modifikasi data valid dari record store dan terjadi proses perbandingan antara password untuk modifikasi data valid dengan password untuk modifikasi data kini. Bila cocok, proses akan menyimpan password untuk modifikasi data terbaru ke dalam record store.

3.3.3 DFD Level 2

DFD Level 2 menggambarkan rincian masing-masing proses yang terdapat dalam DFD Level 1.

3.3.3.1 DFD Level 2 Proses Verifikasi Password



Gambar 3.5 DFD Level 2 Proses Verifikasi Password

Proses 1.1

Proses 1.1 Pembacaan Password dari Record Store memperoleh data input berupa password aplikasi kini. Data tersebut diproses sehingga menjadi data password aplikasi kini (*cipher text*). Data output berupa password aplikasi kini (*cipher text*).

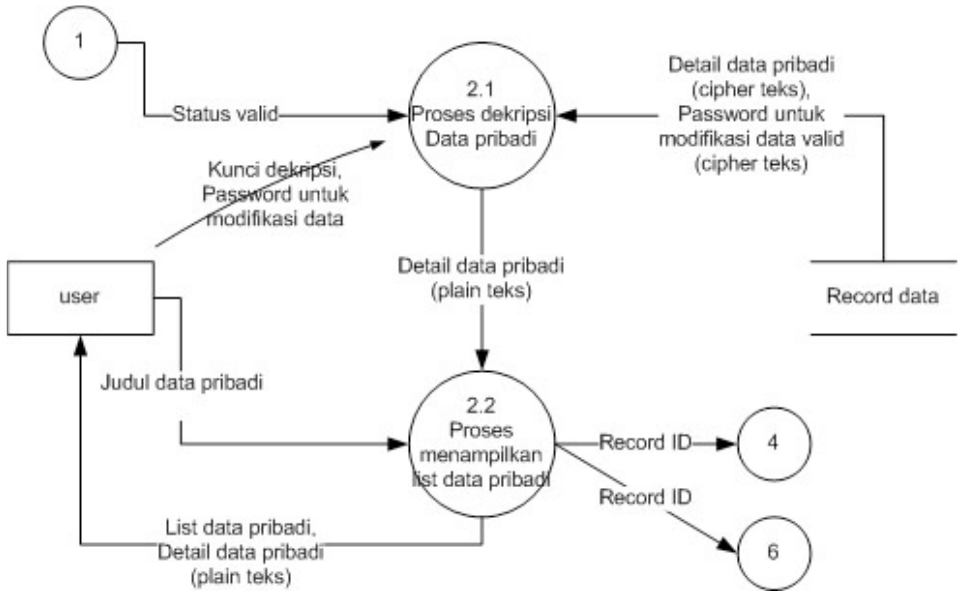
Proses 1.2

Proses 1.2 Pembacaan Password dari Record Store memperoleh data input berupa password aplikasi valid dari record store. Data tersebut diproses sehingga menjadi data password aplikasi valid (*cipher text*). Data output berupa password aplikasi valid (*cipher text*)

Proses 1.3

Proses 1.3 Pencocokan Password menerima data input berupa password aplikasi kini (*cipher text*) dan password aplikasi valid (*cipher text*). Kedua data tersebut diproses sehingga menghasilkan status valid dan konfirmasi verifikasi password. Data output berupa konfirmasi verifikasi password.

3.3.3.2 DFD Level 2 Proses Membaca Data Pribadi



Gambar 3.6 DFD Level 2 Proses Membaca Data Pribadi

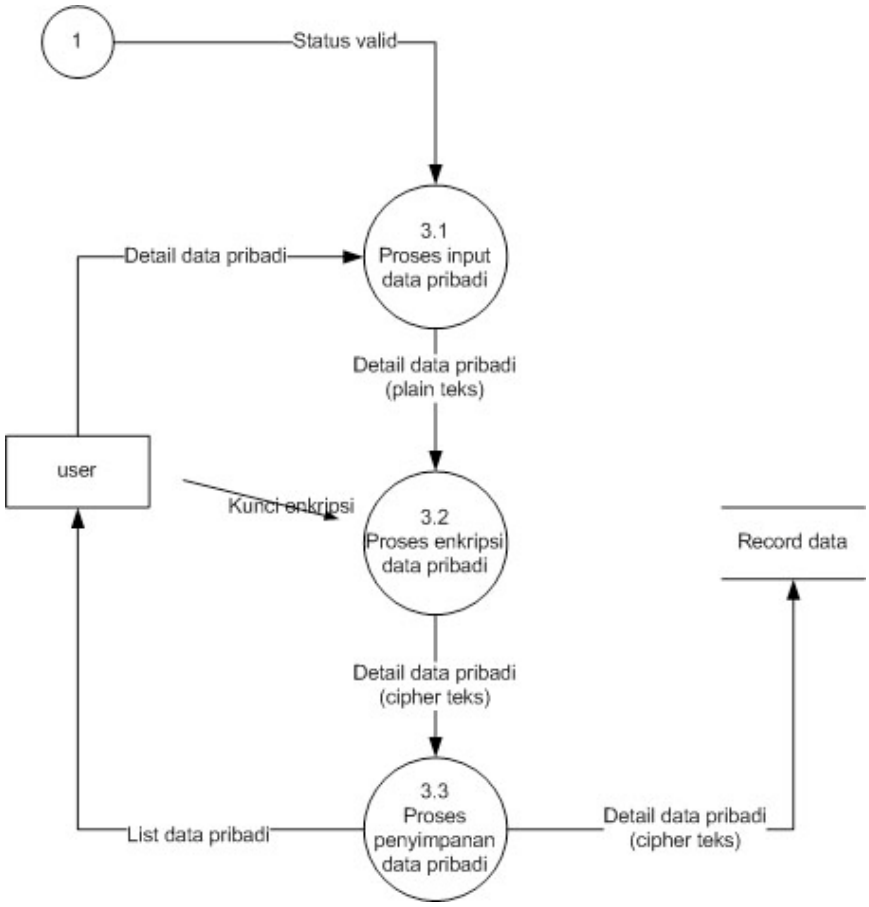
Proses 2.1

Proses 2.1 Dekripsi Data Pribadi memperoleh input data dari proses 1, kunci dekripsi dari user, dan dari record data berupa detail data pribadi terenkripsi, dan mendekripsikan detail data pribadi tersebut menjadi *plain text*. Data output berupa detail data pribadi (*plain text*).

Proses 2.2

Proses 2.2 Menampilkan List Data Pribadi memperoleh input data berupa detail data pribadi dalam bentuk *plain text*, dan menampilkannya ke *user*. *User* dapat membaca detail data pribadi dari daftar data pribadi tersebut data output berupa list data pribadi dan detail data pribadi dalam bentuk *plain text*.

3.3.3.3 DFD Level 2 Proses Menambah Data Pribadi



Gambar 3.7 DFD Level 2 Proses Menambah Data Pribadi

Proses 3.1

Proses 3.1 Input Data Pribadi memperoleh input dari *user* berupa detail data pribadi (judul, tanggal, jenis, isi data pribadi). Data tersebut akan divalidasi dan dibawa ke proses 3.2 Enkripsi Data Pribadi. Data output berupa detail data pribadi dalam bentuk *plain text*.

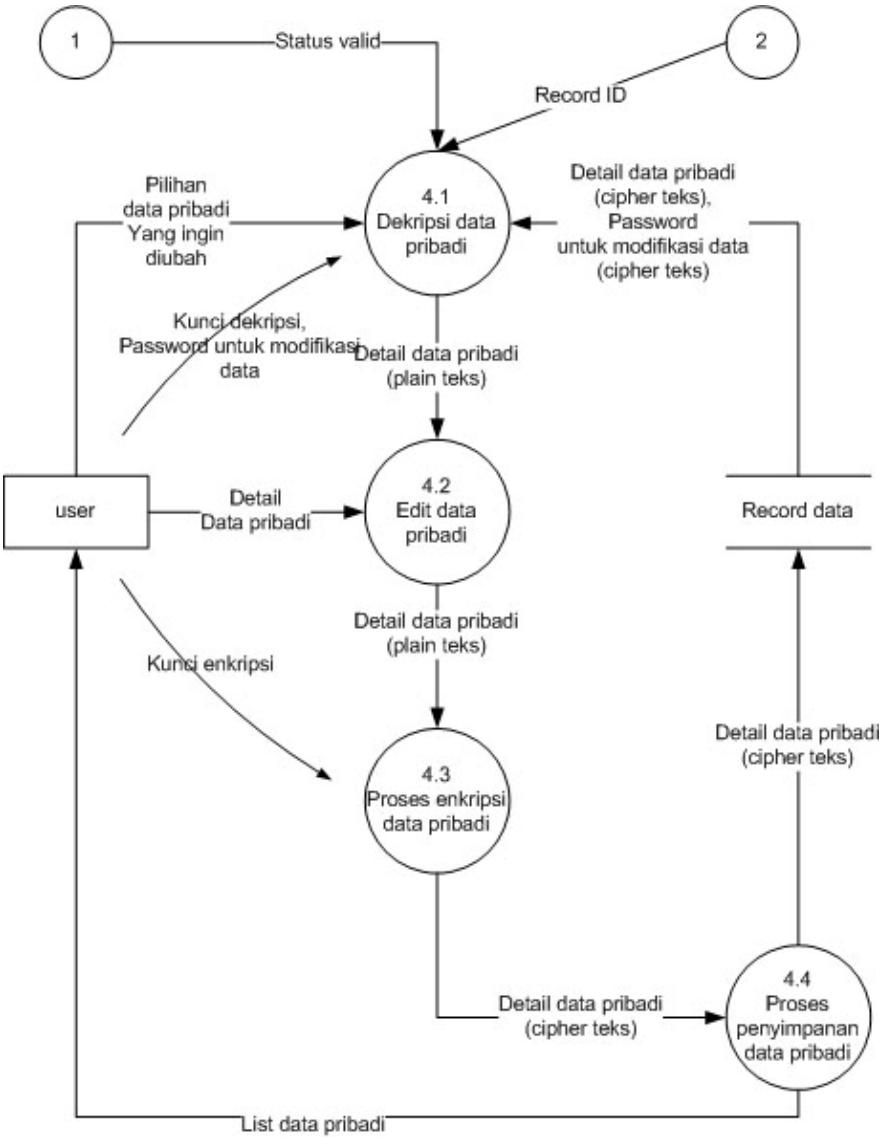
Proses 3.2

Proses 3.2 Enkripsi Data Pribadi mengenkripsi detail data pribadi yang telah divalidasi oleh proses sebelumnya. Data pribadi tersebut akan mengalami proses enkripsi dengan menggunakan kunci enkripsi dari user. Data output berupa detail data pribadi terenkripsi.

Proses 3.3

Proses 3.3 Penyimpanan Data Pribadi menerima input data berupa detail data pribadi terenkripsi. Proses akan menyimpan detail data pribadi tersebut ke record store. Data output berupa detail data pribadi dalam bentuk *plain text*.

3.3.3.4 DFD Level 2 Proses Modifikasi Data Pribadi



Gambar 3.8 DFD Level 2 Proses Modifikasi Data Pribadi

Proses 4.1

Proses 4.1 Dekripsi Data Pribadi memperoleh status valid dari proses sebelumnya, kunci dekripsi dari user, pilihan data pribadi yang ingin diubah dari *user*, record ID dari proses 2 dan detail data pribadi terenkripsi dari record data. Proses akan mendekripsikan detail data pribadi tersebut menjadi detail data pribadi (*cipher text*). Output data berupa detail data pribadi dalam bentuk *plain text*.

Proses 4.2

Proses 4.2 Edit Data Pribadi memperoleh data input berupa detail data pribadi tersebut dan detail data pribadi yang terbaru dari *user*. Proses akan memvalidasi detail data pribadi tersebut. Data output berupa detail data pribadi yang telah dimodifikasi tetapi masih dalam bentuk *plain text*.

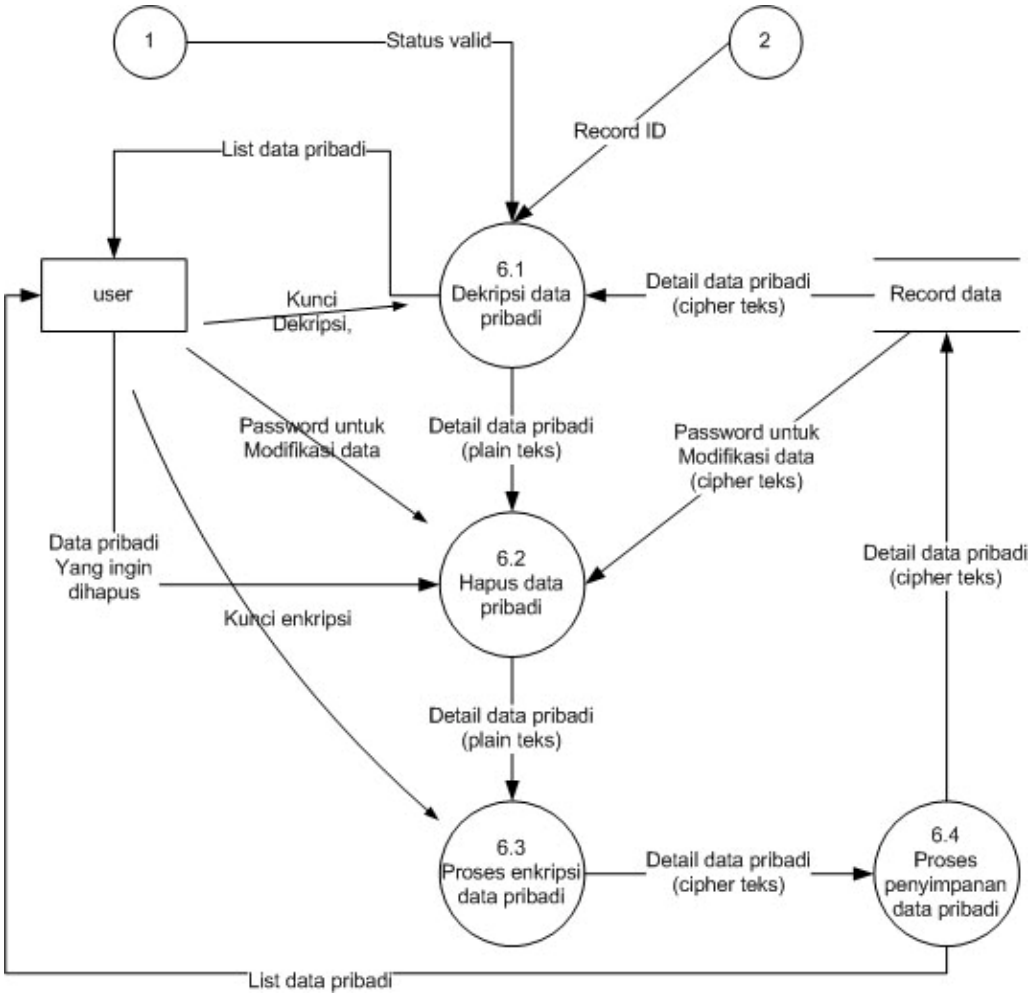
Proses 4.3

Proses 4.3 Enkripsi Data Pribadi mengenkripsikan detail data pribadi yang masih dalam bentuk *plain text* dengan menggunakan kunci enkripsi dari user. Proses akan mengenkripsi detail data pribadi tersebut dan menghasilkan detail data pribadi terenkripsi. Data output berupa detail data pribadi dalam bentuk *cipher text*.

Proses 4.4

Proses 4.4 Penyimpanan Data Pribadi menerima data input dari proses 3.1 berupa detail data pribadi (*cipher text*). Proses akan melakukan penyimpanan detail data pribadi (*cipher text*) tersebut ke dalam record store. Data output berupa detail data pribadi dalam bentuk *cipher text*.

3.3.3.5 DFD Level 2 Proses Menghapus Data Pribadi



Gambar 3.9 DFD Level 2 Proses Menghapus Data Pribadi

Proses 6.1

Proses 6.1 Dekripsi Data Pribadi memperoleh status valid dari proses sebelumnya,record ID dari proses 2, kunci dekripsi dari user dan detail data pribadi terenkripsi dari record data. Proses akan mendekripsikan detail data pribadi tersebut menjadi. Data output berupa detail data pribadi dalam bentuk *plain text*.

Proses 6.2

Proses 6.2 Hapus Data Pribadi memperoleh data input berupa detail data pribadi dan pilihan data pribadi yang ingin dihapus. Proses akan menghapus detail data pribadi yang telah dipilih tersebut. Data output berupa detail data pribadi terbaru tetapi belum mengalami proses enkripsi.

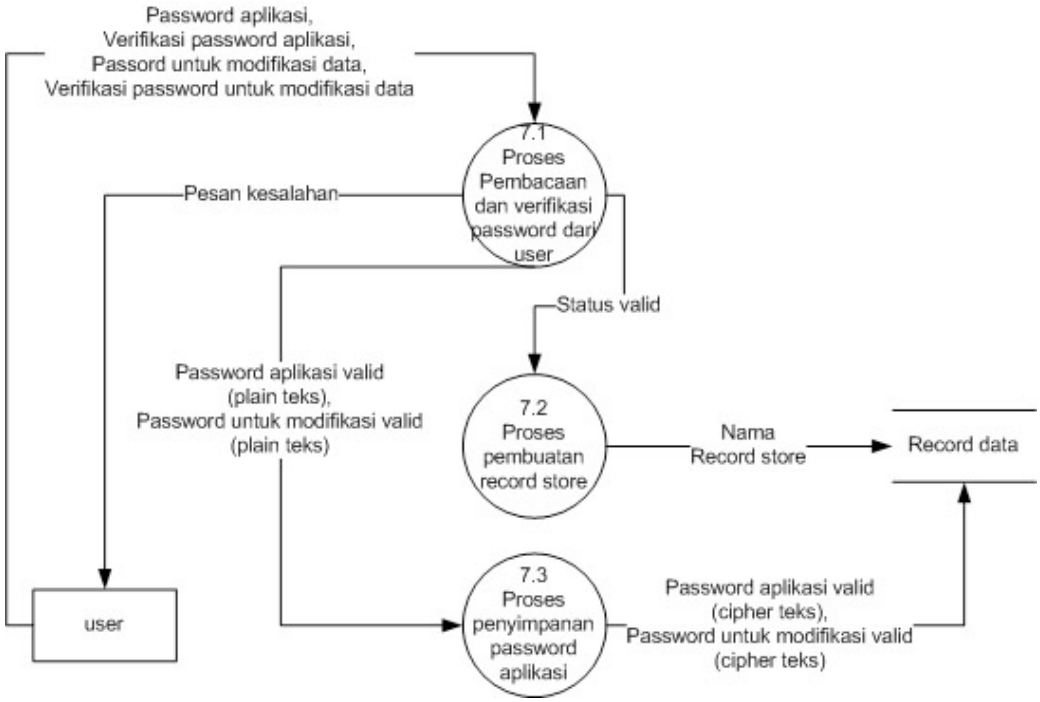
Proses 6.3

Proses 6.3 Enkripsi Data Pribadi mengenkripsikan detail data pribadi yang masih dalam bentuk *plain text* dengan menggunakan kunci enkripsi dari user dan menghasilkan detail data pribadi terenkripsi. Data output berupa detail data pribadi dalam bentuk *cipher text*.

Proses 6.4

Proses 6.4 Penyimpanan Data Pribadi menyimpan detail data pribadi terenkripsi ke dalam record store.

3.3.3.6 DFD Level 2 Proses Setting Password Aplikasi



Gambar 3.10 DFD Level 2 Proses Setting Password Aplikasi

Proses 7.1

Proses 7.1 Pembacaan dan Verifikasi Password dari User menerima data input dari user berupa password aplikasi dan verifikasi password aplikasi beserta password untuk modifikasi data dan verifikasi password untuk modifikasi data. Proses akan mengecek keempat data tersebut dan bila kedua data tersebut adalah sama, proses akan menghasilkan data output berupa status valid dan informasi password aplikasi valid dan password untuk modifikasi data valid dalam bentuk *plain text*. Bila kedua data tersebut adalah tidak sama, proses akan memberikan pesan kesalahan ke user.

Proses 7.2

Proses 7.2 Pembuatan Record Store menerima data input dari proses 7.1 berupa status valid. Selanjutnya proses akan menciptakan suatu record store di dalam ponsel.

Proses 7.3

Proses 7.3 Penyimpanan Password Aplikasi menerima data input dari proses 7.1 berupa informasi password aplikasi valid (*plain text*) dan password untuk modifikasi data valid (*plain text*). Proses menenkripsi informasi data password tersebut dan menghasilkan informasi berupa password aplikasi valid (*cipher text*) beserta password untuk modifikasi data valid (*cipher text*) dan menyimpannya ke dalam record store.

BAB 4 DESKRIPSI PERANCANGAN

4.1 Deskripsi Data

Deskripsi Data menjelaskan data yang digunakan dalam aplikasi Secure Notes. Terdapat tiga macam data yaitu Password Aplikasi, Password untuk Modifikasi Data dan Detail Data Pribadi.
Deskripsi data yang digunakan dalam aplikasi Secure Notes bisa dilihat pada Tabel 4.1.

Tabel 4.1 Deskripsi Data Aplikasi Secure Notes

No	Nama Data	Tipe Data	Keterangan

1	Password Aplikasi	String	Password aplikasi yang diberikan user untuk proses autentikasi aplikasi.
			Password Aplikasi dienkripsi dengan menggunakan algoritma kriptografi MD5.
			
			Contoh :
			Password Aplikasi :
			`SecureNotes`
			Hasil enkripsi :
			`dcffe4257609e9df2f980ab481c6674a`

2	Password untuk Modifikasi Data	String	Password yang diperlukan untuk memodifikasi data pribadi yang telah ada.
			Password untuk Modifikasi Data dienkripsi dengan menggunakan algoritma kriptografi MD5.
			
			Contoh :
			Password untuk Modifikasi Data :
			`SecureNotes`
			Hasil enkripsi :
			`dcffe4257609e9df2f980ab481c6674a`

3	Detail data pribadi	String	Detail data pribadi terdiri atas judul, kategori, waktu, dan isi data pribadi yang selanjutnya akan dienkripsi atau didekripsi
			Detail data pribadi dienkripsi dengan menggunakan algoritma kriptografi RC4.
			
			Contoh Detail Data Pribadi:
			Judul Data Pribadi (100 karakter)
			`Catatan rekening bank Mandiri`
			Kategori Data Pribadi
			`Business`
			Isi Data Pribadi (1000 karakter)
			`No rekening: 1090004967154`
			`No PIN : 1234`
			Kunci Enkripsi (100 karakter)

4.2 Dekomposisi Fungsional Modul

Deksripsi Fungsional Modul menjelaskan daftar input-proses-output aplikasi Secure Notes.
Pemaparan fungsional modul pada aplikasi Secure Notes bisa dilihat pada Tabel 4.2.

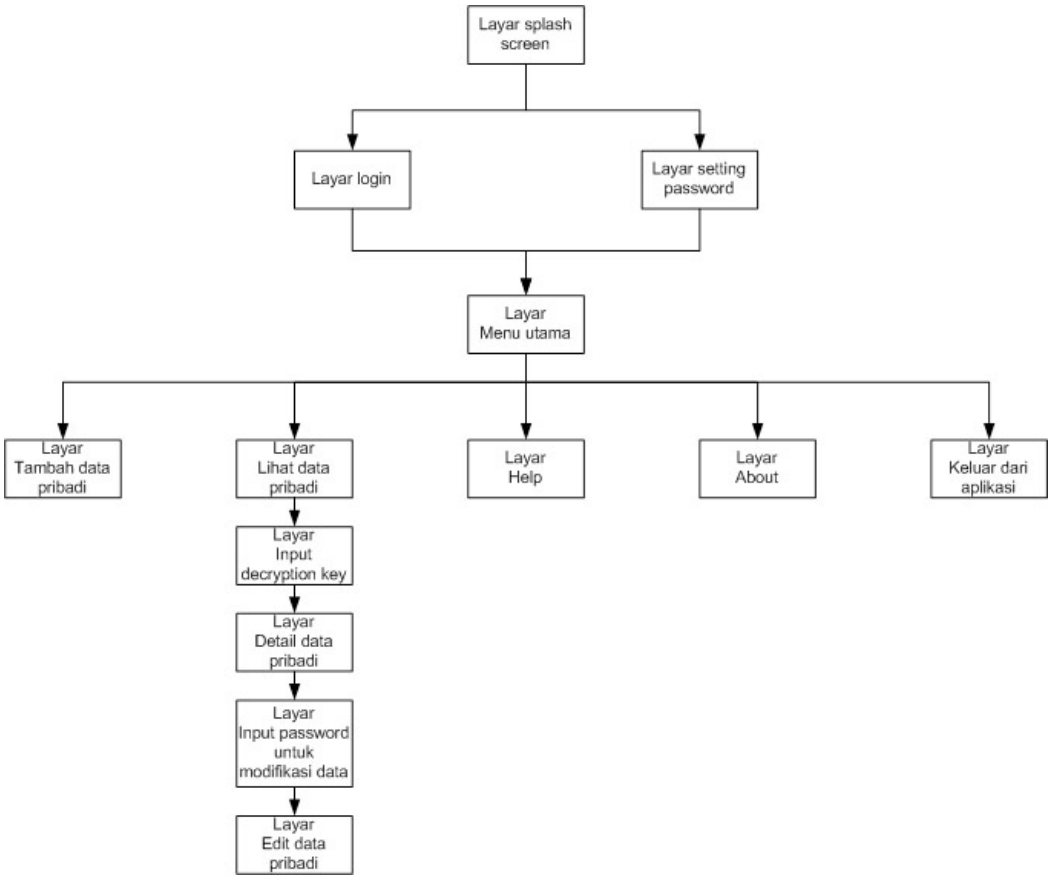
No .	No Fungsi	Proses	Record Input	Data Input	Record Output	Data Output	Ket
1.	F1.1	Proses pembacaan password dari user	-	Password aplikasi kini	-	Password aplikasi kini (*cipher text*)	
2.	F1.2	Proses pembacaan password dari record store	Record data	Password aplikasi valid	-	Password aplikasi valid (*cipher text*)	
3.	F1.3	Proses pencocokan password	-	Password aplikasi kini (*cipher text*)	-	Konfirmasi verifikasi password, status valid	
4.	F2.1	Proses dekripsi data pribadi	Record data	Status valid, kunci dekripsi, detail data pribadi (*cipher text*)	-	Detail data pribadi (*plain text*)	
5.	F2.2	Proses menampilkan list data pribadi	-	Judul data pribadi, detail data pribadi (*plain text*)	-	Record ID,List data pribadi, detail data pribadi (*plain text*)	
6.	F3.1	Proses input data pribadi	-	Status valid, detail data pribadi	-	Detail data pribadi (*plain text*)	
7.	F3.2	Proses enkripsi data pribadi	-	Kunci enkripsi, detail data pribadi (*plain text*)	-	Detail data pribadi (*cipher text*)	
8.	F3.3	Proses penyimpanan data pribadi	-	Detail data pribadi (*cipher texy*)	Record data	Detail data pribadi (*cipher text*)	
9.	F4.1	Proses dekripsi data pribadi	Record data	Status valid, record ID, detail data pribadi (*cipher text*), kunci dekripsi, pilihan data pribadi yang ingin diubah	-	Detail data pribadi (*plain text*)	
10.	F4.2	Proses edit data pribadi	-	Detail data pribadi (*plain text*), detail data pribadi	-	Detail data pribadi (*plain text*)	

No .	No Fungsi	Proses	Record Input	Data Input	Record Output	Data Output	Ket
11.	F4.3	Proses enkripsi data pribadi	-	Detail data pribadi (*plain text*), kunci enkripsi	-	Detail data pribadi (*cipher text*)	
12.	F4.4	Proses penyimpanan data pribadi	-	Detail data pribadi (*cipher text*)	Record data	Detail data pribadi (*cipher text*)	
13.	F5	Proses modifikasi password aplikasi	Record data	Status valid, password aplikasi kini, password aplikasi baru	Record data	Password aplikasi baru	
14.	F6.1	Proses dekripsi data pribadi	Record data	Status valid, record ID, kunci dekripsi, Detail data pribadi (*cipher text*)	-	List data pribadi, detail data pribadi (*plain text*)	
15.	F6.2	Proses hapus data pribadi	-	Data pribadi yang ingin dihapus, detail data pribadi (*plain text*)	-	Detail data pribadi (*plain text*)	
16.	F6.3	Proses enkripsi data pribadi	-	Detail data pribadi (*plain text*), kunci enkripsi	-	Detail data pribadi (*cipher text*)	
17.	F6.4	Proses penyimpanan data pribadi	-	Detail data pribadi (*cipher text*)	Record data	Detail data pribadi (*cipher text*)	
18.	F7.1	Proses Pembacaan dan verifikasi password dari user	-	Password aplikasi, verifikasi password aplikasi	-	Status valid	
19.	F7.2	Proses pembuatan record store	-	Status valid	Record data	Nama record store	
20.	F7.3	Proses penyimpanan password aplikasi	-	Password aplikasi valid (*plain text*)	Record data	Password aplikasi valid (*cipher text*)	
21.	F8	Proses modifikasi password untuk modifikasi data	Record data	Status valid, password kini, password terbaru	Record data	Password untuk modifikasi data yang terbaru	

Tabel 4.2 Deskripsi IPO (Input-Proses-Output) Aplikasi Secure Notes

4.3 Spesifikasi Kebergantungan Antar Layar

Spesifikasi ketergantungan antar layar menjelaskan ketergantungan antar layar yang terdapat dalam aplikasi Secure Notes.
Spesifikasi ketergantungan antar layar aplikasi Secure Notes bisa dilihat pada Gambar 4.1.



Gambar 4.1 Spesifikasi Ketergantungan Antar Layar Aplikasi Secure Notes

4.4 Struktur Menu

Struktur menu aplikasi Secure Notes digambarkan sebagai berikut:

```
Aplikasi Secure Notes  ---Login       ---Main Menu
                                             ---     Create New Notes
                                             ---     See All Notes
                                             ---     Change Application Password
                                             ---     Change Password for Modify Data
                                             ---     Help
                                             ---     About
                                             ---     Exit
```

Gambar 4.2 Struktur Menu Aplikasi Secure Notes

BAB 5 IMPLEMENTASI DAN PENGUJIAN

5.1 Library yang Digunakan

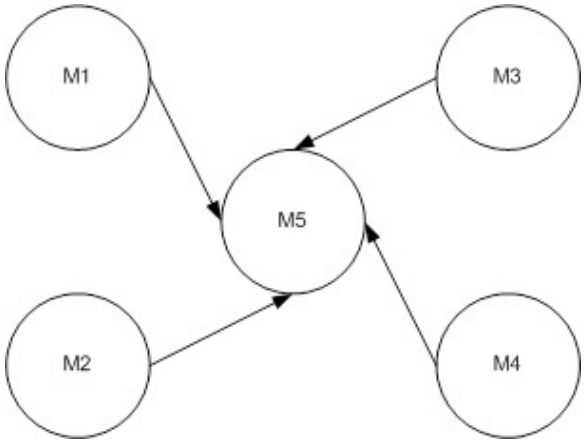
Setelah dilakukan tahap perancangan aplikasi, maka tahap selanjutnya adalah tahap Implementasi dan Pengujian.
Tahap implementasi merupakan tahap dimana setiap fungsi yang telah dirancang sebelumnya diimplementasikan ke dalam bahasa pemrograman, yang dalam hal ini menggunakan bahasa *JAVA2 for Mobile Edition (J2ME).* Sedangkan tahap pengujian merupakan tahap dimana fungsi-fungsi yang telah diimplementasikan tersebut diuji, apakah telah sesuai dengan dekripsi perancangan aplikasi atau tidak.

5.2 Spesifikasi Kebergantungan Antar Modul

Spesifikasi Kebergantungan Antar Modul menjelaskan kebergantungan antar modul yang ada dalam aplikasi Secure Notes.
Aplikasi Secure Notes memiliki 5 modul yaitu :

1. Modul enkripsi-dekripsi dengan RC4 (M1)
2. Modul *hashing* dengan MD5 (M2)
3. Modul *password* (M3)
4. Modul *record store* (M4)
5. Modul *MIDlet* (M5)

Masing-masing modul berada dalam satu *file class*.
Spesifikasi kebergantungan antar modul dapat dilihat pada Gambar 5.1



Gambar 5.1 Spesifikasi Kebergantungan Antar Modul Aplikasi Secure Notes

5.3 Struktur Direktori dan Deskripsi File

Struktur Direktori dan Deskripsi File menjelaskan tentang struktur direktori dan pengumpulan fungsi menjadi file pada Aplikasi Secure Notes.
Struktur direktori dan deskripsi file aplikasi Secure Notes dapat dilihat pada Tabel 5.1

Tabel 5.1 Struktur Direktori dan Deskripsi File Aplikasi Secure Notes

Nama Direktori	Nama File	Nama Modul	Nama Fungsi	Keterangan

SecureNotes	RC4Engine.java	Modul enkripsi-dekripsi dengan RC4	`init()`
			`processBytes()`
			`bytesToHex()`
				Pustaka kriptografi dengan algoritma RC4

SecureNotes	MD5Digest.java	Modul *hashing*	`calculate()`	Pustaka kriptografi

Nama Direktori	Nama File	Nama Modul	Nama Fungsi	Keterangan
		dengan MD5		dengan algoritma MD5

SecureNotes	HexCodec.java	Modul enkripsi-dekripsi dengan RC4	`bytesToHex()`
			`hexToBytes()`
			`hexToBytes()`	

SecureNotes	PasswordRecord.java	Modul *password*	`openRecordData()`
			`entriPasswd()`
			`editPasswd()`
			`setPasswd()`
			`setNewPasswd()`
			`readPasswd()`
			`getTfOldPass()`
			`getTfPass1()`
			`getTfPass2()`
			`setTfOldPass()`
			`setTfPass1()`
			`setTfPass2()`	

SecureNotes	DataRecord.java	Modul *record store*	`openRecordData()`
			`cekRecordData()`
			`addNewNotes()`
			`viewNotes()`
			`getNotesID()`
			`getTitleByID()`
			`getCategoryByID()`
			`getDetailByID()`
			`deleteNotes()`
			`encryption()`
			`decryption()`	

SecureNotes	SecureNotes.java	Modul *MIDlet*	`initialize()`
			`getDisplay()`
			`exitMIDlet()`
			`startApp()`
			`pauseApp()`
			`destroyApp()`
			`entriPasswd()`
			`entriData()`
			`editData()`
			`tampilListDataPribadi()`
			`mainMenu()`
			`splashScreen()`
			`commandAction()`	

5.4 Pengujian dan Hasilnya

Setelah dilakukan implementasi fungsi, maka selanjutnya adalah melakukan pengujian terhadap fungsi-fungsi seperti pada Tabel 5.1.
Rincian pengujian dan hasilnya dapat dilihat pada Lampiran D : Dokumen Rinci Pengujian.

BAB 6 KESIMPULAN DAN SARAN

Setelah aplikasi Secure Notes selesai diimplementasikan dan telah melalui tahap pengujian maka dapat dihasilkan kesimpulan dan saran mengenai aplikasi tersebut.

6.1 Kesimpulan

Kesimpulan yang dapat diambil dari pengembangan aplikasi Secure Notes adalah sebagai berikut:

- Aplikasi Secure Notes dapat digunakan untuk menyimpan pribadi dan rahasia di ponsel secara persisten dengan aman
- Dari 20 fungsi yang direncanakan terdapat 20 fungsi yang telah diimplementasi dan diuji coba.
- Jenis ponsel yang dapat menggunakan aplikasi Secure Notes adalah ponsel dengan profile MIDP 2.0. Aplikasi Secure Notes telah diimplementasikan pada ponsel Nokia 3110c, Nokia 5300, Nokia 6300, Nokia N70 dan Sony Ericsson W880i dan memberikan hasil yang sama.

6.2 Saran

Saran atas pengembangan aplikasi Secure Notes adalah sebagai berikut:

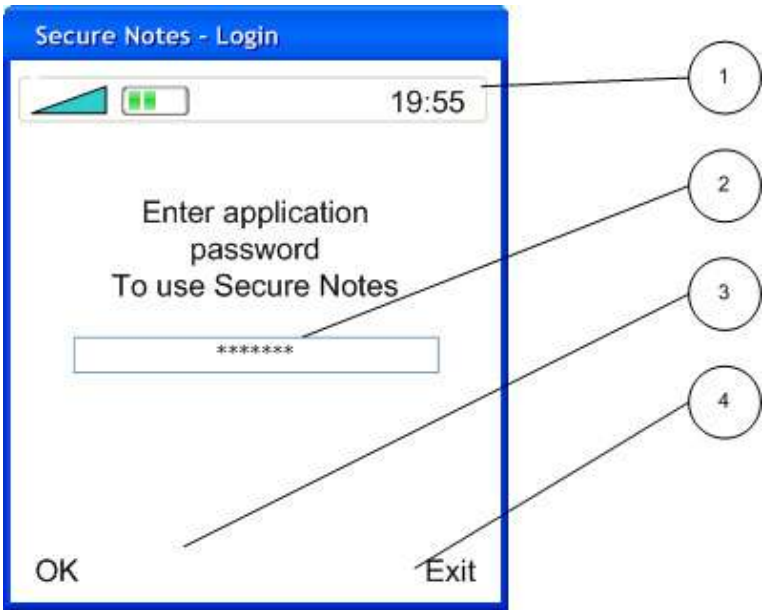
- Aplikasi dapat mengirim data pribadi ke ponsel lain supaya pengguna yang memiliki lebih dari satu ponsel dapat mengirim data pribadinya yang ada pada ponsel yang satu ke ponsel yang lainnya.

LAMPIRAN A PERANCANGAN RINCI FUNGSIONAL

A.1 Spesifikasi Fungsi / Proses F1.1

Identifikasi / Nama : F1.1
Deskripsi Isi : Proses pembacaan password dari user
Jenis : Form Entry-Columnar

A.1.1 Spesifikasi Layar Utama



A.1.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Textfield	Tempat masukan password aplikasi
3	Command	Left softkey
4	Command	Right softkey

A.1.3 Spesifikasi Layar Pesan

Tidak ada

A.1.4 Spesifikasi Proses / Algoritma

Initial state Textfield belum terisi
Final state Password aplikasi dari user telah dienkripsi
Algoritma PasswordAplikasiKini ← Textfield2 PasswordAplikasiKiniCipher ← PasswordAplikasiKini dienkripsi dengan algoritma MD5

A.1.5 Spesifikasi Report

Tidak ada

A.2 Spesifikasi Fungsi / Proses F1.2

Identifikasi / Nama : F1.2
Deskripsi Isi : Proses pembacaan password dari record store
Jenis : Proses tanpa layar

A.2.1 Spesifikasi Layar Utama

Tidak ada

A.2.2 Spesifikasi Objek-Objek pada Layar

Tidak ada

A.2.3 Spesifikasi Layar Pesan

Tidak ada

A.2.4 Spesifikasi Proses / Algoritma

Initial state Record data belum dibaca oleh aplikasi
Final state Record data telah dibaca oleh aplikasi
Algoritma **//password aplikasi yang disimpan dalam record data berupa data terenkripsi** **//password aplikasi dienkripsi dengan algoritma MD5** PasswordAplikasiValidCipher ← baca dari record data

A.2.5 Spesifikasi Report

Tidak ada

A.3 Spesifikasi Fungsi / Proses F1.3

Identifikasi / Nama : F1.3
Deskripsi Isi : Proses pencocokan password
Jenis : Proses tanpa layar

A.3.1 Spesifikasi Layar Utama

Tidak ada

A.3.2 Spesifikasi Objek-Objek pada Layar

Tidak ada

A.3.3 Spesifikasi Layar Pesan

Tidak ada

A.3.4 Spesifikasi Proses / Algoritma

```
Initial state
Password dari user dan password dari record store belum dibandingkan
Final state
Login diterima atau ditolak
Algoritma
  If PasswordAplikasiKiniCipher = PasswordAplikasiValidCipher Then
    Login diterima
    Status Valid
  Else
    Login ditolak
    Panggil proses F1.1
  End If
```

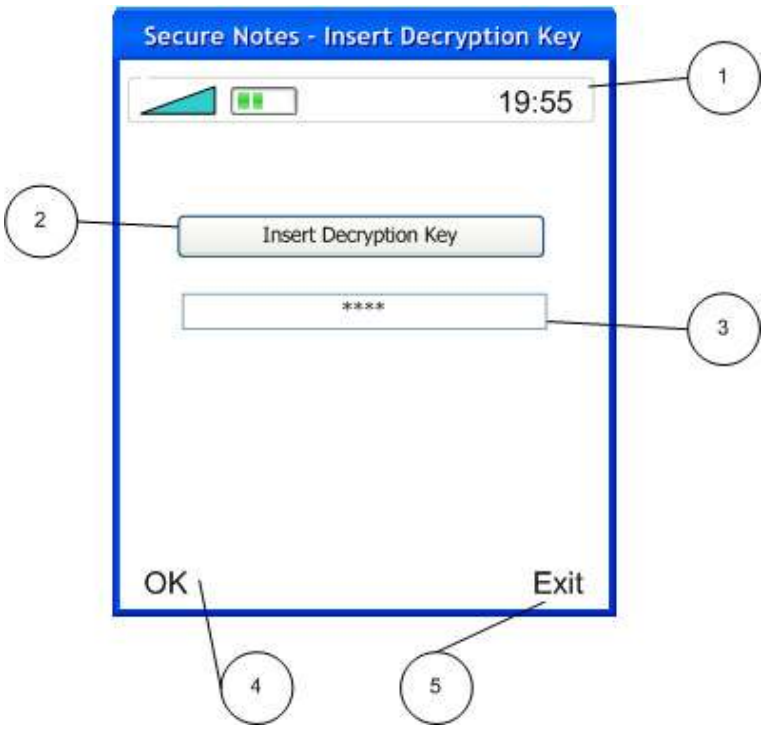
A.3.5 Spesifikasi Report

Tidak ada

A.4 Spesifikasi Fungsi / Proses F2.1

Identifikasi / Nama : F2.1
Deskripsi Isi : Proses dekripsi data pribadi
Jenis : Form Entry-Columnar

A.4.1 Spesifikasi Layar Utama



A.4.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label kunci dekripsi
3	Textfield	Tempat masukan kunci dekripsi
4	Command	Left softkey

ID Objek	Jenis	Keterangan
5	Command	Right softkey

A.4.3 Spesifikasi Layar Pesan

Tidak ada

A.4.4 Spesifikasi Proses / Algoritma

```
Initial state
Detail data pribadi belum didekripsi
Final state
Detail data pribadi telah didekripsi
Algoritma
  //DecryptionKey digunakan untuk proses dekripsi
  DecryptionKey ← enkripsi PassAplikasiValid dengan algoritma MD5

  DetailDataPribadiCipher ← baca dari record store
  DetailDataPribadiPlain ← dekripsi DetailDataPribadiCipher dengan algoritma RC4
```

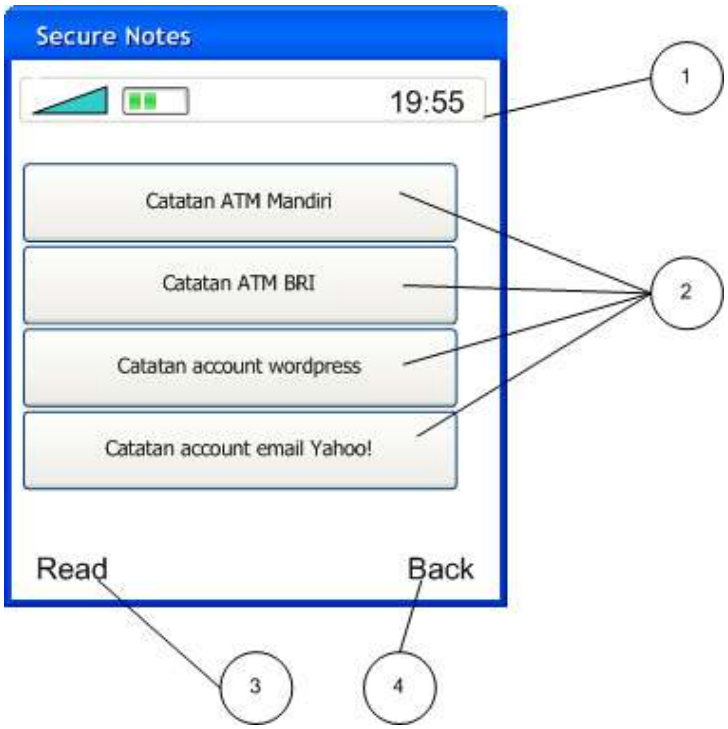
A.4.5 Spesifikasi Report

Tidak ada

A.5 Spesifikasi Fungsi / Proses F2.2

Identifikasi / Nama : F2.2
Deskripsi Isi : Proses menampilkan list data pribadi
Jenis : Master-Detail

A.5.1 Spesifikasi Layar Utama



A.5.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	List	Daftar judul detail data pribadi yang telah ada
3	Command	Left softkey
4	Command	Right softkey

A.5.3 Spesifikasi Layar Pesan

Tidak ada

A.5.4 Spesifikasi Proses / Algoritma

Initial state

```
Tampilan layar daftar detail data pribadi dalam bentuk List
```

Final state

```
Tampil data pribadi sesuai dengan pilihan user
```

Algoritma

```
  DetailDataPribadiPlain ← dekripsi DetailDataPribadiCipher dengan algoritma RC4
  While Masih ada data pribadi dalam DetailDataPribadiPlain
     Membaca judul data pribadi
     Dekripsi judul data pribadi dengan algoritma RC4
     Menampilkan judul data pribadi ke layer ponsel
  End While

  JudulDataPribadi ← pilihan dari user
  Tampilkan DetailDataPribadiPlain sesuai dengan judul pilihan user
  Record_ID ← nomor record dari detail data pribadi pilihan user
```

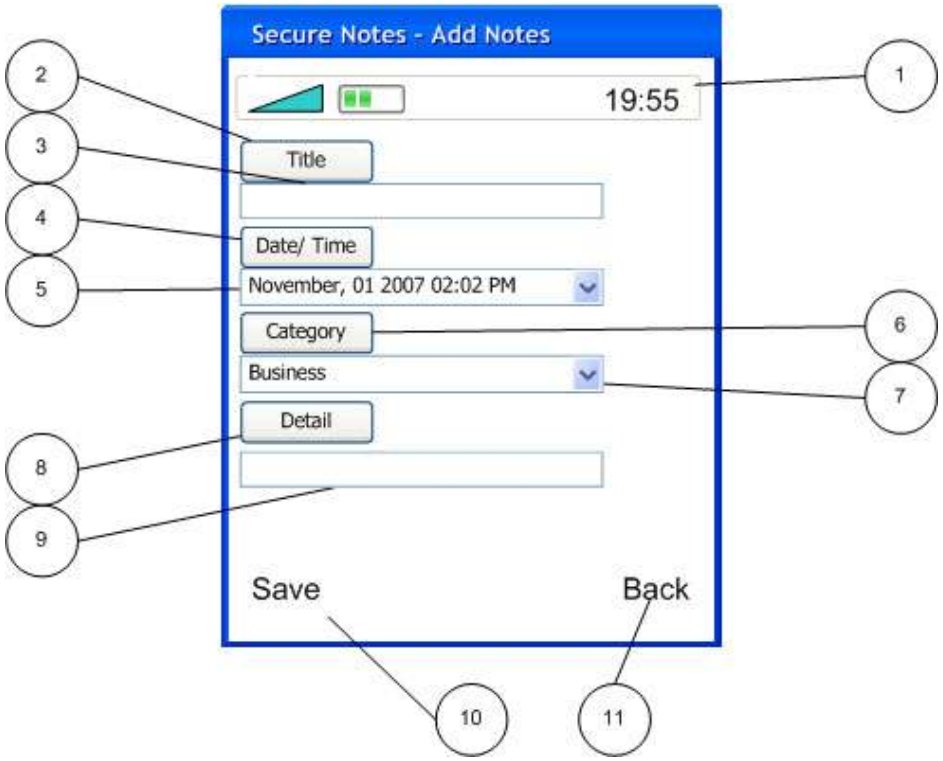
A.5.5 Spesifikasi Report

Tidak ada

A.6 Spesifikasi Fungsi / Proses F3.1

Identifikasi / Nama : F3.1
Deskripsi Isi : Proses input data pribadi
Jenis : Form Entry-Columnar

A.6.1 Spesifikasi Layar Utama



A.6.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label judul data pribadi
3	Textfield	Keterangan judul data pribadi
4	Label	Label tanggal dan dan waktu pembuatan data pribadi
5	Combobox	Keterangan tanggal dan waktu pembuatan data pribadi
6	Label	Label kategori data pribadi
7	Combobox	Keterangan kategori data pribadi
8	Label	Label isi data pribadi
9	Textfield	Keterangan isi data pribadi
10	Command	Left softkey
11	Command	Right softkey

A.6.3 Spesifikasi Layar Pesan

Tidak ada

A.6.4 Spesifikasi Proses / Algoritma

Initial state

Muncul layer input data pribadi

Final state

User menekan tombol softkey kiri

Algoritma

```
  JudulDataPribadi ← Textfield3
  WaktuPembuatanDataPribadi ← Textfield5
  KategoriDataPribadi ← Textfield7
  IsiDataPribadi ← Textfield9

  If Command10 di tekan then
            Panggil proses F3.2
  Else If Command11 di tekan then
```

```
            Kembali ke layar menu utama
  Else
  End If
```

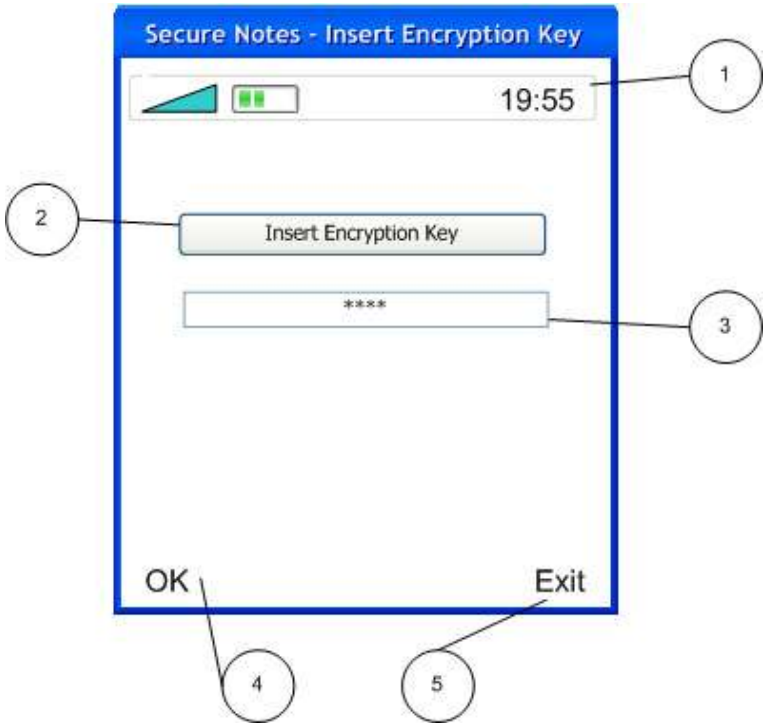
A.6.5 Spesifikasi Report

Tidak ada

A.7 Spesifikasi Fungsi / Proses F3.2

Identifikasi / Nama : F3.2
Deskripsi Isi : Proses enkripsi data pribadi
Jenis : Form Entry-Columnar

A.7.1 Spesifikasi Layar Utama



A.7.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label kunci enkripsi
3	Textfield	Tempat masukan kunci enkripsi
4	Command	Left softkey
5	Command	Right softkey

A.7.3 Spesifikasi Layar Pesan

Tidak ada

A.7.4 Spesifikasi Proses / Algoritma

Initial state Data pribadi belum dienkripsi
Final state Daata pribadi telah dienkripsi
Algoritma **//EncryptionKey digunakan untuk proses enkripsi** EncryptionKey ← enkripsi PassAplikasiValid dengan algoritma MD5 DetailDataPribadiPlain ← inputan dari proses F3.1 DetailDataPribadiCipher ← DetailDataPribadiPlain dienkripsi dengan algoritma RC4

A.7.5 Spesifikasi Report

Tidak ada

A.8 Spesifikasi Fungsi / Proses F3.3

Identifikasi / Nama : F3.3
Deskripsi Isi : Proses penyimpanan data pribadi
Jenis : Proses tanpa layar

A.8.1 Spesifikasi Layar Utama

Tidak ada

A.8.2 Spesifikasi Objek-Objek pada Layar

Tidak ada

A.8.3 Spesifikasi Layar Pesan

Tidak ada

A.8.4 Spesifikasi Proses / Algoritma

Initial state Data pribadi telah dienkripsi
Final state Data pribadi telah disimpan dalam record store
Algoritma DetailDataPribadiCipher ← DetailDataPribadiPlain dienkripsi dengan algoritma RC4 DetailDataPribadiCipher disimpan ke dalam record data Panggil proses F2.2

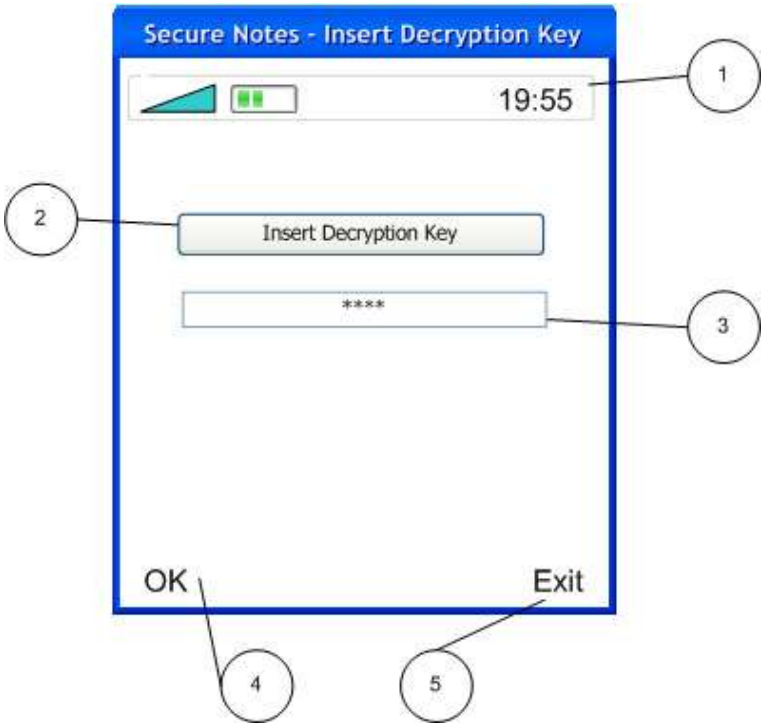
A.8.5 Spesifikasi Report

Tidak ada

A.9 Spesifikasi Fungsi / Proses F4.1

Identifikasi / Nama : F4.1
Deskripsi Isi : Proses dekripsi data pribadi
Jenis : Form Entry-Columnar

A.9.1 Spesifikasi Layar Utama



A.9.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label kunci dekripsi
3	Textfield	Tempat masukan kunci dekripsi
4	Command	Left softkey
5	Command	Right softkey

A.9.3 Spesifikasi Layar Pesan

Tidak ada

A.9.4 Spesifikasi Proses / Algoritma

```
Initial state
Data pribadi belum dibaca dari record store
Final state
Data pribadi telah dibaca dari record store
Algoritma
  //DecryptionKey digunakan untuk proses dekripsi
  DecryptionKey ← enkripsi PassAplikasiValid dengan algoritma MD5

  DetailDataPribadiCipher ← baca dari record store
  DetailDataPribadiPlain ← dekripsi DetailDataPribadiCipher dengan algoritma RC4
```

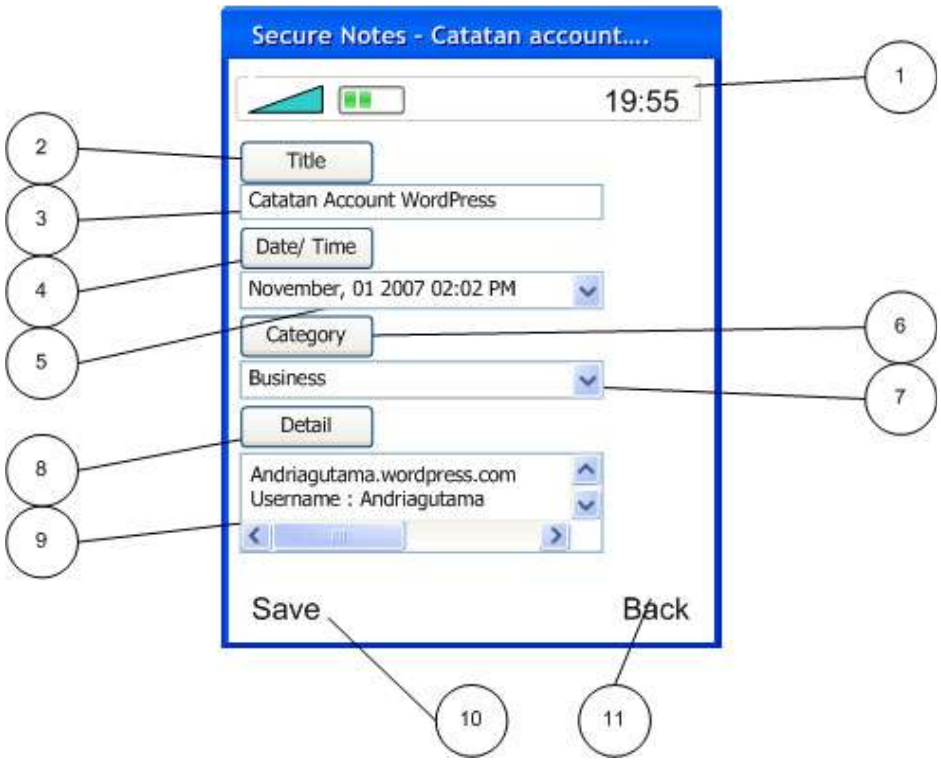
A.9.5 Spesifikasi Report

Tidak ada

A.10 Spesifikasi Fungsi / Proses F4.2

Identifikasi / Nama : F4.2
Deskripsi Isi : Proses edit data pribadi
Jenis : Form Entry-Columnar

A.10.1 Spesifikasi Layar Utama



A.10.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label judul data pribadi
3	Textfield	Keterangan judul data pribadi
4	Label	Label tanggal dan dan waktu pembuatan data pribadi
5	Combobox	Keterangan tanggal dan waktu pembuatan data pribadi
6	Label	Label kategori data pribadi
7	Combobox	Keterangan kategori data pribadi
8	Label	Label isi data pribadi
9	Textfield	Keterangan isi data pribadi
10	Command	Left softkey
11	Command	Right softkey

A.10.3 Spesifikasi Layar Pesan

Tidak ada

A.10.4 Spesifikasi Proses / Algoritma

Initial state Data pribadi telah didekripsi
Final state User menekan tombol softkey kiri
Algoritma

```
JudulDataPribadi ← Textfield3
WaktuPembuatanDataPribadi ← Textfield5
KategoriDataPribadi ← Textfield7
IsiDataPribadi ← Textfield9

If Command10 di tekan then
        Panggil proses F4.3
Else If Command11 di tekan then
        Kembali ke layar proses F2.2
Else
End If
```

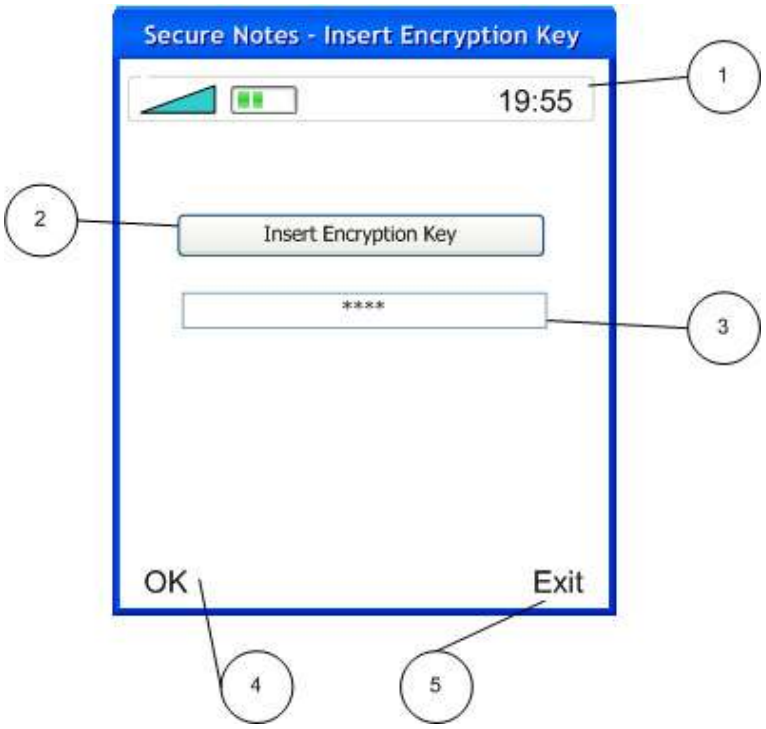
A.10.5Spesifikasi Report

Tidak ada

A.11 Spesifikasi Fungsi / Proses F4.3

Identifikasi / Nama : F4.3
Deskripsi Isi : Proses enkripsi data pribadi
Jenis : Form Entry-Columnar

A.11.1Spesifikasi Layar Utama



A.11.2Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label kunci enkripsi
3	Textfield	Tempat masukan kunci enkripsi
4	Command	Left softkey
5	Command	Right softkey

A.11.3Spesifikasi Layar Pesan

Tidak ada

A.11.4Spesifikasi Proses / Algoritma

Initial state Data pribadi belum dienkripsi
Final state Data pribadi telah dienkripsi
Algoritma **//EncryptionKey digunakan untuk proses enkripsi** EncryptionKey ← enkripsi PassAplikasiValid dengan algoritma MD5 DetailDataPribadiPlain ← inputan dari proses F3.1 DetailDataPribadiCipher ← DetailDataPribadiPlain dienkripsi dengan algoritma RC4

A.11.5Spesifikasi Report

Tidak ada

A.12 Spesifikasi Fungsi / Proses F4.4

Identifikasi / Nama : F4.4
Deskripsi Isi : Proses penyimpanan data pribadi
Jenis : Proses tanpa layar

A.12.1Spesifikasi Layar Utama

Tidak ada

A.12.2Spesifikasi Objek-Objek pada Layar

Tidak ada

A.12.3Spesifikasi Layar Pesan

Tidak ada

A.12.4Spesifikasi Proses / Algoritma

Initial state Data pribadi belum disimpan dalam record store
Final state Data pribadi telah disimpan dalam record store
Algoritma DetailDataPribadiCipher ← DetailDataPribadiPlain dienkripsi dengan algoritma RC4 DetailDataPribadiCipher disimpan ke dalam record data Panggil proses F2.2

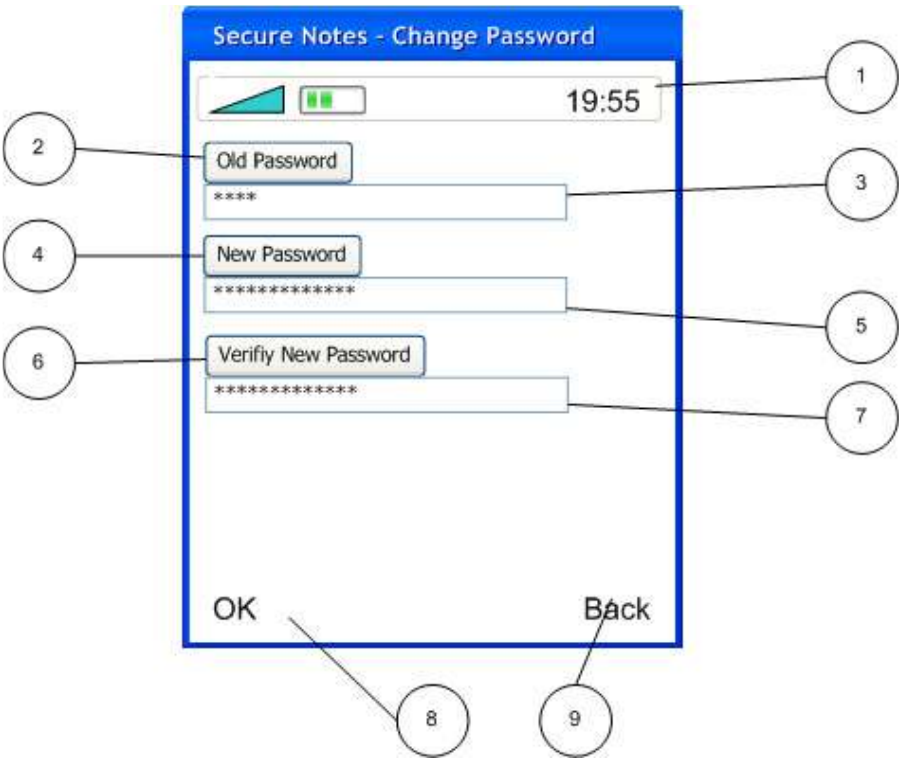
A.12.5Spesifikasi Report

Tidak ada

A.13 Spesifikasi Fungsi / Proses F5

Identifikasi / Nama : F5
Deskripsi Isi : Proses modifikasi password aplikasi
Jenis : Form Entry-Columnar

A.13.1 Spesifikasi Layar Utama



A.13.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label password lama
3	Textfield	Tempat masukan password lama
4	Label	Label password baru
5	Textfield	Tempat masukan password baru
6	Label	Label password baru
7	Textfield	Tempat masukan password baru
8	Command	Left softkey
9	Command	Right softkey

A.13.3 Spesifikasi Layar Pesan

No	Kasus	Pesan
1	Password aplikasi tidak sesuai	“Password Incorrect”
2	Password aplikasi baru dan verifikasi tidak sesuai	“New Password and Verify Password Doesn’t Match”

A.13.4 Spesifikasi Proses / Algoritma

Initial state
Muncul layar mengganti password aplikasi
Final state

```
Password aplikasi berhasil diubah dan disimpan dalam record data
Algoritma
        PassAplikasiValidCipher ← data password yang dibaca dari record data
        PassAplikasi ← Textfield3
        PassAplikasiCipher ← PassAplikasi dienkripsi dengan algoritma MD5
        PassAplikasiBaru ← Textfield5
        PassAplikasiVerify ← Textfield7
        PassAplikasiBaruCipher ← PassAplikasiBaru dienkripsi dengan algoritma MD5
        If Command8 di tekan then
            If PassAplikasiCipher == PassAplikasiValidCipher then
                        If PassAplikasiBaru == PassAplikasiVerifiy
                                Simpan data password terbaru ke record data
                        Else
                                Tampil layar pesan2
                        End If
            Else
                        Tampil layar pesan2
            End If
        Else If Command9 di tekan then
            Kembali ke layar menu utama
        Else
        End If
```

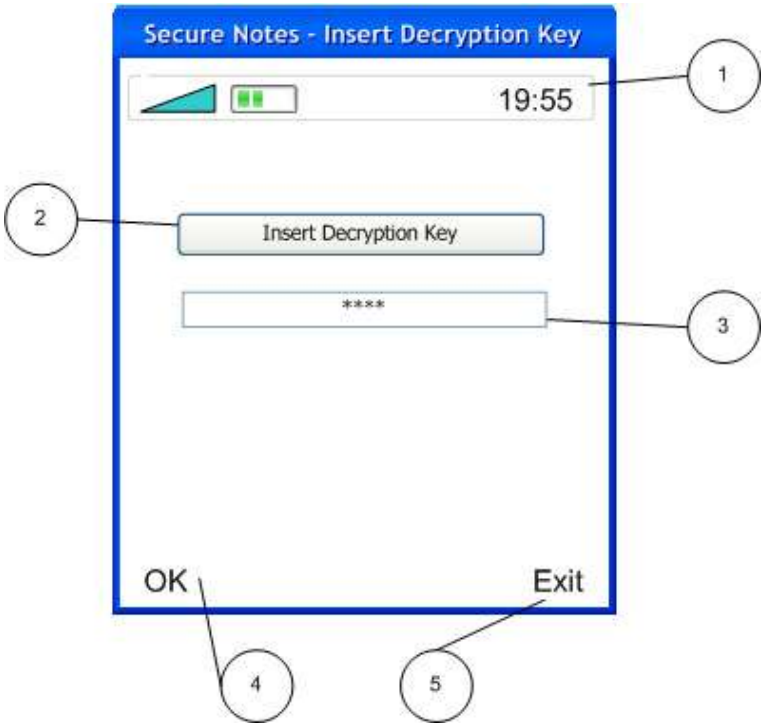
A.13.5Spesifikasi Report

Tidak ada

A.14 Spesifikasi Fungsi / Proses F6.1

Identifikasi / Nama : F6.1
Deskripsi Isi : Proses dekripsi data pribadi
Jenis : Form Entry-Columnar

A.14.1Spesifikasi Layar Utama



A.14.2Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label kunci dekripsi
3	Textfield	Tempat masukan kunci dekripsi
4	Command	Left softkey
5	Command	Right softkey

A.14.3Spesifikasi Layar Pesan

Tidak ada

A.14.4Spesifikasi Proses / Algoritma

```
Initial state
Data pribadi belum dibaca dari record store
Final state
Data pribadi telah didekripsi
Algoritma
  //DecryptionKey digunakan untuk proses dekripsi
  DecryptionKey ← enkripsi PassAplikasiValid dengan algoritma MD5

  DetailDataPribadiCipher ← baca dari record store
  DetailDataPribadiPlain ← dekripsi DetailDataPribadiCipher dengan algoritma RC4
  Panggil proses F2.2
```

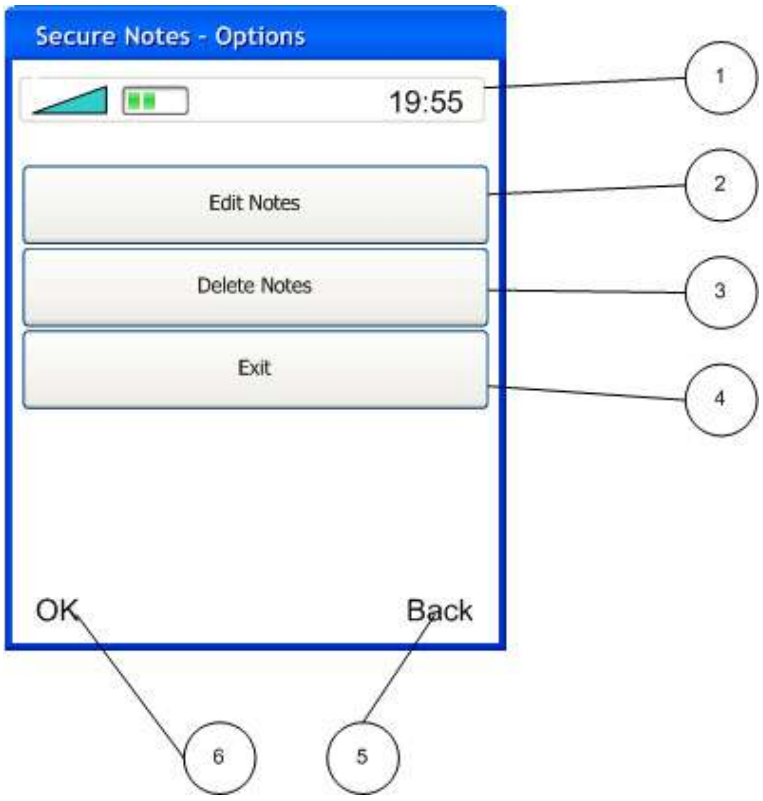
A.14.5Spesifikasi Report

Tidak ada

A.15 Spesifikasi Fungsi / Proses F6.2

Identifikasi / Nama : F6.2
Deskripsi Isi : Proses hapus data pribadi
Jenis : Master-Detail

A.15.1Spesifikasi Layar Utama



A.15.2Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	List	Pilihan menu edit data pribadi
3	List	Pilihan menu hapus data pribadi
4	Command	Right softkey
5	Command	Left softkey

A.15.3Spesifikasi Layar Pesan

Tidak ada

A.15.4Spesifikasi Proses / Algoritma

Initial state

Data pribadi belum dihapus

Final state

Data pribadi telah dihapus

Algoritma

```
If Command5 di tekan then
          Panggil proses F6.1
          Menghapus data pribadi yang terpilih
          Panggil proses F6.4
Else If Command4 di tekan then
          Kembali ke layar F2.2
Else
End If
```

A.15.5Spesifikasi Report

Tidak ada

A.16 Spesifikasi Fungsi / Proses F6.3

Identifikasi / Nama : F6.3
Deskripsi Isi : Proses enkripsi data pribadi
Jenis : Proses tanpa layar

A.16.1Spesifikasi Layar Utama

Tidak ada

A.16.2Spesifikasi Objek-Objek pada Layar

Tidak ada

A.16.3Spesifikasi Layar Pesan

Tidak ada

A.16.4Spesifikasi Proses / Algoritma

```
Initial state
Data pribadi belum dienkripsi
Final state
Data pribadi telah dienkripsi
Algoritma
  //EncryptionKey digunakan untuk proses enkripsi
  EncryptionKey ← enkripsi PassAplikasiValid dengan algoritma MD5

  DetailDataPribadiPlain ← inputan dari proses F6.2
  DetailDataPribadiCipher ← DetailDataPribadiPlain dienkripsi dengan algoritma RC4
```

A.16.5Spesifikasi Report

Tidak ada

A.17 Spesifikasi Fungsi / Proses F6.4

Identifikasi / Nama : F6.4
Deskripsi Isi : Proses penyimpanan data pribadi
Jenis : Proses tanpa layar

A.17.1Spesifikasi Layar Utama

Tidak ada

A.17.2Spesifikasi Objek-Objek pada Layar

Tidak ada

A.17.3Spesifikasi Layar Pesan

Tidak ada

A.17.4Spesifikasi Proses / Algoritma

Initial state Data pribadi belum disimpan ke dalam record store
Final state Data pribadi telah disimpan ke dalam record store
Algoritma DetailDataPribadiCipher ← DetailDataPribadiPlain dienkripsi dengan algoritma RC4 DetailDataPribadiCipher disimpan ke dalam record data Panggil proses F2.2

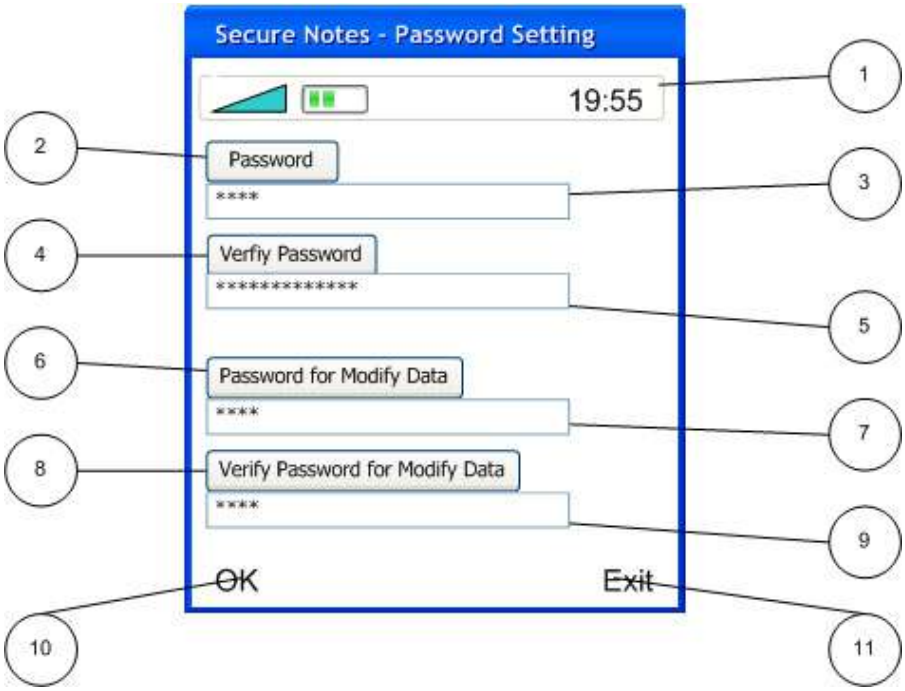
A.17.5Spesifikasi Report

Tidak ada

A.18 Spesifikasi Fungsi / Proses F7.1

Identifikasi / Nama : F7.1
Deskripsi Isi : Proses Pembacaan dan verifikasi password dari user
Jenis : Form Entry-Columnar

A.18.1Spesifikasi Layar Utama



A.18.2Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label password aplikasi
3	TextField	Tempat masukan password aplikasi
4	Label	Label verifikasi password aplikasi
5	TextField	Tempat masukan verifikasi password aplikasi
6	Label	Label masukan password untuk modifikasi data
7	TextField	Tempat masukan password untuk modifikasi data
8	Label	Label verifikasi password untuk modifikasi data

ID Objek	Jenis	Keterangan
9	TextField	Tempat masukan verifikasi password untuk modifikasi data
10	Command	Left softkey
11	Command	Right softkey

A.18.3Spesifikasi Layar Pesan

No	Kasus	Pesan
1	Password aplikasi tidak sama dengan verifikasi password aplikasi, atau Password untuk modifikasi data tidak sama dengan verifikasi password untuk modifikasi data	"Password Doesn't match with Verify Password, or Password for Modify Data doesn't Match with Verify Password for Modify Data"

A.18.4Spesifikasi Proses / Algoritma

Initial state

```
Textfield belum terisi
```

Final state

```
User menekan tombol left softkey
```

Algoritma

```
  String passAplikasi ← TextField3
  String passAplikasiVerify ← TextField5
  String passForModifyData ← TextField7
  String passForModifyDataVerify ← TextField9
  If command6 ditekan then
    If passAplikasi == passAplikasiVerfiy AND passForModifyData ==
passForModifyDataVerify Then
      Panggil proses 7.2
    Else
      Muncul layar pesan1
      Panggil proses 7.1
    End If
  Else If command7 ditekan then
    Keluar dari aplikasi
  End If
```

A.18.5Spesifikasi Report

Tidak ada

A.19 Spesifikasi Fungsi / Proses F7.2

Identifikasi / Nama : F7.2
Deskripsi Isi : Proses pembuatan record store
Jenis : Proses tanpa layar

A.19.1Spesifikasi Layar Utama

Tidak ada

A.19.2Spesifikasi Objek-Objek pada Layar

Tidak ada

A.19.3Spesifikasi Layar Pesan

Tidak ada

A.19.4 Spesifikasi Proses / Algoritma

Initial state Record store belum diciptakan
Final state Record store telah diciptakan
Algoritma Menciptakan sebuah record store

A.19.5 Spesifikasi Report

Tidak ada

A.20 Spesifikasi Fungsi / Proses F7.3

Identifikasi / Nama : F7.3
Deskripsi Isi : Proses penyimpanan password aplikasi
Jenis : Proses tanpa layar

A.20.1 Spesifikasi Layar Utama

Tidak ada

A.20.2 Spesifikasi Objek-Objek pada Layar

Tidak ada

A.20.3 Spesifikasi Layar Pesan

Tidak ada

A.20.4 Spesifikasi Proses / Algoritma

Initial state Informasi password aplikasi valid belum disimpan ke dalam record store
Final state Informasi password aplikasi valid telah disimpan ke dalam record store
Algoritma passAplikasiValid ← dari proses 7.1 passForModifyDataValid ← dari proses 7.1 passAplikasiValidCipher ← enkripsi passAplikasiValid dengan algoritma MD5 passForModifyDataValidCipher ← enkripsi passForModifyDataValid dengan MD5 simpan passAplikasiValidCipher ke record data simpan passForModifyDataValidCipher ke record data

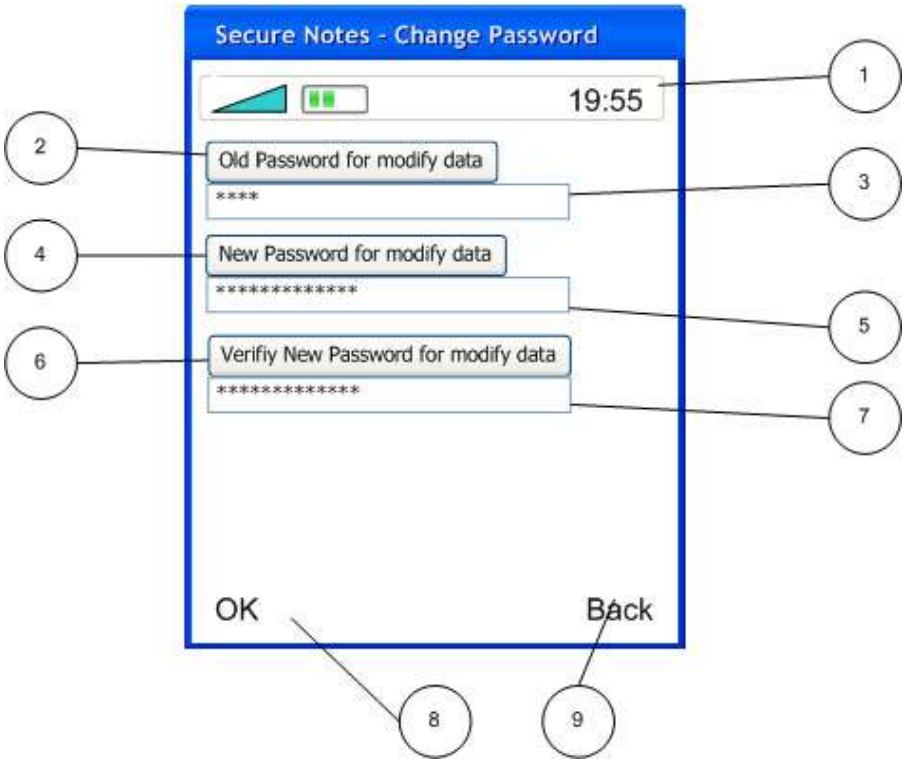
A.20.5 Spesifikasi Report

Tidak ada

A.21 Spesifikasi Fungsi / Proses F8

Identifikasi / Nama : F8
Deskripsi Isi : Proses modifikasi password untuk modifikasi data
Jenis : Form Entry-Columnar

A.21.1 Spesifikasi Layar Utama



A.21.2 Spesifikasi Objek-Objek pada Layar

ID Objek	Jenis	Keterangan
1	Label	Indikator baterai, sinyal dan keterangan waktu
2	Label	Label password untuk modifikasi data lama
3	Textfield	Tempat masukan password untuk modifikasi data lama
4	Label	Label password untuk modifikasi data baru
5	Textfield	Tempat masukan untuk modifikasi data password baru
6	Label	Label password untuk modifikasi data baru
7	Textfield	Tempat masukan untuk modifikasi data password baru
8	Command	Left softkey
9	Command	Right softkey

A.21.3 Spesifikasi Layar Pesan

No	Kasus	Pesan
1	Password untuk modifikasi data tidak sesuai	"Password For Modify DataIncorrect"
2	Password untuk modifikasi data dan verifikasi tidak sesuai	"New Password For Modify Data and Verify Password Doesn't Match"

A.21.4 Spesifikasi Proses / Algoritma

Initial state

```
Muncul layar mengganti password aplikasi
```

Final state

```
Password aplikasi berhasil diubah dan disimpan dalam record data
```

Algoritma

```
PassForModifyDataValidCipher ← data password yang dibaca dari record data
PassForModifyData ← Textfield3
PassForModifyDataCipher ← PassForModifyData dienkripsi dengan algoritma MD5
```

```
        PassForModifyDataBaru ← Textfield5
        PassForModifyDataVerify ← Textfield7
        PassForModifyDataBaruCipher    ←    PassForModifyDataBaru    dienkripsi    dengan
algoritma MD5
        If Command8 di tekan then
            If PassForModifyDataCipher == ForModifyDataValidCipher then
                        If PassForModifyDataBaru == PassForModifyDataVerifiy
                                 Simpan data password terbaru ke record data
                        Else
                                Tampil layar pesan2
                        End If
            Else
                        Tampil layar pesan2
            End If
        Else If Command9 di tekan then
            Kembali ke layar menu utama
        Else
        End If
```

A.21.5 Spesifikasi Report

Tidak ada

LAMPIRAN B URAIAN RINCI LIBRARY

B.1 Spesifikasi Library MD5

Identifikasi/ Nama : MD5 (*Message Digest 5*)
Deskripsi Isi : *Library* untuk enkripsi data dengan algoritma MD5

MD5 merupakan fungsi *hash* satu arah yang diciptakan oleh Ron Rivest. Fungsi *hash* satu arah adalah dimana kita dengan mudah melakukan enkripsi untuk mendapatkan *cipher text*-nya, tetapi sangat sulit untuk mendapatkan *plain text*-nya.
Alasan penggunaan MD5:

- Algoritma MD5 merupakan algoritma yang sangat sulit dipecahkan karena sifatnya yang satu arah (*one way*)
- Penggunaan algoritma MD5 relatif mudah
- Algoritma MD5 menghasilkan output sepanjang 128bit yang sangat tepat digunakan sebagai kunci enkripsi/ dekripsi

B.1.1 Spesifikasi Fungsi calculate()

Identifikasi/ Nama : `public String calculate(String m)`
Penggunaan : Fungsi ini menghasilkan *cipher text* dari parameter berupa *plain text*

B.2 Spesifikasi Library RC4

Identifikasi/ Nama : RC4 (*Rivest Code 4*)
Deskripsi Isi : *Library* untuk enkripsi-dekripsi data dengan algoritma RC4

RC4 merupakan algoritma kriptografi yang tergolong dalam jenis *Symnetric Algorithm*, atau algoritma kunci simetris. Algoritma kunci simetris adalah algoritma kriptografi di mana untuk proses enkripsi dan dekripsinya memakai kunci yang sama. Algoritma kriptografi RC4 diciptakan oleh Ron Rivest.
Alasan penggunaan RC4:

- Algoritma RC4 merupakan algoritma yang sangat sulit dipecahkan
- Penggunaan algoritma RC4 yang menggunakan kunci 128bit akan memerlukan waktu yang cukup lama untuk dipecahkan sehingga penggunaan RC4 dengan kunci hasil *hashing* sangat disarankan
- Penggunaan algoritma RC4 relatif mudah

Perbandingan tingkat keamanan algoritma kriptografi RC4 bila dibandingkan dengan algoritma kriptografi DES.

Panjang Kunci	Jaminan Waktu untuk Menemukan Kunci (DES)	Jaminan Waktu untuk Menemukan Kunci (RC4)
40 bit	0,4 detik	15 hari
56 bit	7 jam	2.691,49 tahun
64 bit	74 jam 40 menit	689.021,57 tahun
128 bit	157.129.203.952.300.000 tahun	12.710.204.652.610.000.000.000.000 tahun

Catatan : dicoba dengan serangan *Brute-Force*
Sumber : http://www.geocities.com/amwibowo/resource/komparasi/komparasi.html

B.2.1 Spesifikasi Fungsi init()

Identifikasi/ Nama : `public void init(boolean forEncryption,KeyParameter params)`
Penggunaan : Fungsi untuk memulai proses enkripsi atau proses dekripsi

B.2.2 Spesifikasi Fungsi processBytes()

Identifikasi/ Nama : `public void processBytes(byte[] in, int inOff,int len, byte[] out,int outOff)`
Penggunaan : Fungsi enkripsi atau dekripsi

B.2.3 Spesifikasi Fungsi bytesToHex()

Identifikasi/ Nama : `public String bytesToHex(byte[] raw)`
Penggunaan : Fungsi ini merubah tipe data *bytes* menjadi heksadesimal dalam bentuk *String*.

LAMPIRAN C DAFTAR RINCI FILE DAN DATA

C.1 Struktur Direktori

C.1.1 Direktori Pengembangan

Direktori Pengembangan adalah direktori yang berhubungan dengan tahap pengembangan aplikasi Secure Notes. Direktori Pengembangan terdiri atas dua subdirektori yaitu subdirektori Source Code dan subdirektori Dokumentasi.

- Source Code, berisi source code aplikasi Secure Notes
- Dokumentasi, berisi semua dokumen aplikasi Secure Notes

C.1.2 Direktori Operasional

Direktori Operasional adalah direktori yang berhubungan dengan tahap implementasi aplikasi Secure Notes. Direktori Operasional terdiri atas satu subdirektori yaitu subdirektori ExeFiles.

- ExeFiles, berisi file executable aplikasi Secure Notes yang selanjutnya diimplementasikan ke ponsel yang sesuai

C.2 Isi Direktori Pengembangan

- Source Code, berisi source code aplikasi Secure Notes
- Dokumentasi, berisi semua dokumen aplikasi Secure Notes

C.2.1 Isi Subdirektori Pengembangan/Source Code

```
Directory of D:\POLITEKNIK_BATAM\TA\Pengembangan\Source Code

06/12/2007  11:46    <DIR>          .
06/12/2007  11:46    <DIR>          ..
06/12/2007  11:46    <DIR>          SecureNotes
               0 File(s)              0 bytes
               3 Dir(s)  59.956.994.048 bytes free

Directory of D:\POLITEKNIK_BATAM\TA\Pengembangan\Source Code\SecureNotes

06/12/2007  11:46    <DIR>          .
06/12/2007  11:46    <DIR>          ..
06/12/2007  11:46    <DIR>          build
27/11/2007  22:27             3.560 build.xml
06/12/2007  11:46    <DIR>          dist
06/12/2007  11:46    <DIR>          nbproject
06/12/2007  11:46    <DIR>          src
               1 File(s)          3.560 bytes
               6 Dir(s)  59.956.989.952 bytes free

Directory of
D:\POLITEKNIK_BATAM\TA_2007-2008\TA\Pengembangan\Source Code\SecureNotes\src

12/12/2007  13:36    <DIR>          .
12/12/2007  13:36    <DIR>          ..
12/12/2007  13:36    <DIR>          icons
12/12/2007  13:36    <DIR>          SecureNotes
               0 File(s)              0 bytes
               4 Dir(s)  59.356.741.632 bytes free
```

```
Directory of
D:\POLITEKNIK_BATAM\TA_20072008\TA\Pengembangan\SourceCode\SecureNotes\src\
SecureNotes

12/12/2007  13:36    <DIR>          .
12/12/2007  13:36    <DIR>          ..
12/12/2007  12:39             1.119 About.java
12/12/2007  12:39            19.735 DataRecord.java
12/12/2007  12:39             1.241 Help.java
12/12/2007  12:39             1.293 HexCodec.java
12/12/2007  12:39             8.803 MD5Digest.java
12/12/2007  12:39             7.564 PasswordRecord.java
12/12/2007  12:39             2.971 RC4Engine.java
12/12/2007  12:39            24.308 SecureNotes.java
12/12/2007  12:39               611 SecureNotes.mvd
               9 File(s)         67.645 bytes
               2 Dir(s)  59.356.688.384 bytes free
```

C.2.2 Isi Subdirektori Pengembangan/Dokumentasi

```
Directory of D:\POLITEKNIK_BATAM\TA_2007-2008\SecureNotes\Dokumentasi

22/01/2008  06:32    <DIR>          .
22/01/2008  06:32    <DIR>          ..
31/12/2007  06:33             3.758 algorithm.html
12/12/2007  13:42             3.838 daftarDir.txt
22/01/2008  06:30           752.640 DeskripsiSistem.vsd
28/09/2007  08:20            37.376 logbook_III.doc
28/09/2007  08:19            37.888 logbook_IV.doc
22/11/2007  11:44            41.472 logbook_IX.doc
15/09/2007  10:20            37.376 logbook_I_II.doc
01/11/2007  08:34            40.448 logbook_V.doc
01/11/2007  08:40            40.448 logbook_VI.doc
06/11/2007  07:25            39.424 logbook_VII.doc
16/11/2007  10:53            40.448 logbook_VIII.doc
29/11/2007  07:15            43.008 logbook_X.doc
05/12/2007  17:46            43.008 logbook_XI.doc
14/12/2007  09:39            44.032 logbook_XII.doc
06/12/2007  00:08            40.448 SecureNotes_Bab_I.doc
22/01/2008  06:04            60.928 SecureNotes_Bab_II.doc
22/01/2008  06:23           411.648 SecureNotes_Bab_III.doc
22/10/2007  13:36            36.864 SecureNotes_Bab_III_Cover.doc
22/01/2008  06:31            96.768 SecureNotes_Bab_IV.doc
20/11/2007  10:35            36.864 SecureNotes_Bab_IV_Cover.doc
18/09/2007  08:31            36.864 SecureNotes_Bab_I_II_Cover.doc
22/01/2008  06:31            55.296 SecureNotes_Bab_V.doc
01/01/2008  15:17            41.472 SecureNotes_Bab_VI.doc
06/12/2007  12:12            36.864 SecureNotes_Bab_V_Cover.doc
14/01/2008  09:00         1.460.224 SecureNotes_Buku.doc
14/01/2008  08:54         3.016.704 SecureNotes_Lampiran.doc
22/01/2008  06:24         2.730.496 SecureNotes_Lampiran_A.doc
19/01/2008  13:55            48.640 SecureNotes_Lampiran_B.doc
12/12/2007  13:42            53.248 SecureNotes_Lampiran_C.doc
15/12/2007  07:00            70.144 SecureNotes_Lampiran_D.doc
27/12/2007  09:52            40.960 SecureNotes_Lampiran_E.doc
16/12/2007  13:43            50.688 SecureNotes_Lampiran_F.doc
16/12/2007  14:14            44.544 SecureNotes_Lampiran_G.doc
19/01/2008  13:46           977.920 SecureNotes_Manual.doc
14/01/2008  08:57           442.880 SecureNotes_Pengesahan.doc
              35 File(s)     10.995.628 bytes
               2 Dir(s)  47.998.771.200 bytes free
```

C.3 Isi Direktori Operasional

- ExeFiles, berisi file executable aplikasi Secure Notes yang selanjutnya diimplementasikan ke ponsel yang sesuai

C.3.1 Isi Subdirektori Operasional/ExeFiles

```
Directory of D:\POLITEKNIK_BATAM\TA_2007-2008\TA\Operasional\ExeFiles

12/12/2007  13:41    <DIR>          .
12/12/2007  13:41    <DIR>          ..
12/12/2007  12:45               279 SecureNotes.jad
12/12/2007  12:45            89.704 SecureNotes.jar
               2 File(s)         89.983 bytes
               2 Dir(s)  59.356.622.848 bytes free
```

LAMPIRAN D DOKUMEN RINCI PENGUJIAN

D.1 Tim Penguji

1. Muhammad Wahyudi (MW)
2. Rinaldy (RY)

D.2 Hasil Rinci Pengujian

No	Nama Fungsi	Deskripsi Fungsional	Kelompok Uji	Prosedur dan Kasus Uji	Hasil yang Diharapkan	Hasil Test	Penguji	Tgl Uji	Keterangan
1	F1.1 F1.2 F1.3	Proses pembacaan password dari user	Normal	Memasukkan password benar	Muncul layar menu utama	Diterima	MW	04 Desember 2007	
2	F1.1 F1.2 F1.3	Proses pembacaan password dari user	Data salah	Memasukkan password benar	Tetap pada layar input password	Diterima	MW	04 Desember 2007	
3	F2.1 F2.2	Proses menampilkan list data pribadi	Normal	Memilih menu ‘see all notes’ dari layar menu utama	Tampil list data pribadi	Diterima	MW	06 Desember 2007	
4	F3.1 F3.2 F3.3	Proses input data pribadi	Normal	Memilih menu ‘create new notes’ dari layar menu utama dan selanjutnya mengisi form data pribadi	Data pribadi tersimpan dalam record store	Diterima	MW	06 Desember 2007	
5	F4.1 F4.2 F4.3 F4.4	Proses edit data pribadi	Normal	Memilih salah satu dari list data pribadi, memasukkan key yang sesuai	Data pribadi diedit dan disimpan dalam record store	Diterima	MW	06 Desember 2007	

No	Nama Fungsi	Deskripsi Fungsional	Kelompok Uji	Prosedur dan Kasus Uji	Hasil yang Diharapkan	Hasil Test	Penguji	Tgl Uji	Keterangan
				dan selanjutnya merubah isi data pribadi					
6	F4.1 F4.2 F4.3 F4.4	Proses edit data pribadi	Data salah	Memilih salah satu dari list data pribadi lalu memasukkan key yang tidak sesuai	Data pribadi yang muncul berupa karakter yang tidak terbaca				
7	F5	Proses modifikasi password aplikasi	Normal	Memilih menu ‘change password’ pada menu utama lalu memasukkan password aplikasi yang sebelumnya beserta password aplikasi yang baru	Password aplikasi terganti	Diterima	MW	06 Desember 2007	
8	F5	Proses modifikasi password aplikasi	Data salah	Memilih menu ‘change password’ pada menu utama lalu memasukkan password aplikasi yang tidak sesuai dengan password aplikasi sebelumnya	Muncul layar pesan dan user dibawa kembali pada proses modifikasi password aplikasi	Diterima	MW	06 Desember 2007	

No	Nama Fungsi	Deskripsi Fungsional	Kelompok Uji	Prosedur dan Kasus Uji	Hasil yang Diharapkan	Hasil Test	Penguji	Tgl Uji	Keterangan
9	F6.1 F6.2 F6.3 F6.4	Proses hapus data pribadi	Normal	Memilih opsi 'delete' dari list data pribadi	Data pribadi dhapus	Diterima	MW	06 Desember 2007	
10	F7.1 F7.2 F7.3	Proses setting password aplikasi	Normal	Memasukkan password dan verifikasi password	Password aplikasi telah ditentukan dan muncul layar menu utama	Diterima	MW	06 Desember 2007	
11	F7.1 F7.2 F7.3	Proses setting password aplikasi	Data salah	Memasukkan password yang berbeda dengan verifikasi password	Muncul layar pesan dan user dibawa kembali pada proses setting password aplikasi	Diterima	MW	12 Desember 2007	

LAMPIRAN E FLOW MAP & PROSEDUR

Tidak ada

LAMPIRAN F LOGBOOK

Minggu	Periode	Ada/ Tidak Ada
1 dan 2	3 September s.d. 14 September 2007	Ada
3	17 September s.d. 21 September 2007	Ada
4	24 September s.d. 28 September 2007	Ada
5	22 Oktober s.d. 26 Oktober 2007	Ada
6	29 Oktober s.d. 2 November 2007	Ada
7	5 November s.d. 9 November 2007	Ada
8	12 November s.d. 16 November 2007	Ada
9	19 November s.d. 23 November 2007	Ada
10	26 November s.d 30 November 2007	Ada
11	3 Desember s.d 7 Desember 2007	Ada
12	10 Desember s.d 14 Desember 2007	Ada
13		
14		