APLIKASI OTENTIKASI KONEKSI *BLUETOOTH*

TUGAS AKHIR

Oleh :

Wahyuni Sya'arany 33106121

Disusun untuk memenuhi syarat kelulusan Program Diploma III

PROGRAM STUDI APLIKASI PERANGKAT LUNAK
JURUSAN TEKNIK INFORMATIKA
POLITEKNIK BATAM
BATAM
2009

LEMBAR PENGESAHAN

APLIKASI OTENTIKASI KONEKSI *BLUETOOTH*

TUGAS AKHIR

Oleh :

Wahyuni Sya'arany
33106121

Batam, 3 Agustus 2009

Pembimbing ,

Agus Fatulloh, ST
NIK. 107051

ABSTRAKSI

APLIKASI OTENTIKASI KONEKSI *BLUETOOTH*

Bluetooth merupakan media komunikasi *wireless* yang populer dewasa ini dan banyak digunakan oleh *vendor* perangkat *mobile* sebagai salah satu fasilitas pengiriman data. Namun belum terdapat mekanisme untuk otentikasi pengguna pada komunikasi *Bluetooth,* otentikasi hanya dilakukan pada perangkat, sehingga jika perangkat yang berkomunikasi sama maka dianggap proses komunikasi dilakukan dengan pengguna yang benar.

Terkait hal tersebut, maka dibuatlah suatu aplikasi yang bertujuan untuk memberikan layanan keamanan koneksi *Bluetooth* dengan mengimplementasikan mekanisme pertukaran kunci dengan menggunakan algoritma Diffie-Hellman untuk mempertukarkan kunci rahasia dengan pihak yang otentik untuk mendapatkan kunci privat sebagai pengotentikasi pengguna.

Kata Kunci: *Bluetooth,* Algoritma Diffie-Hellman, koneksi, Handphone

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT atas segala rahmat, hidayah, dan petunjuk-Nya, tak lupa pula Nabi besar Muhammad SAW atas segala suri tauladannya, yang memberikan hidayahnya serta kekuatan sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul Aplikasi Otentikasi Koneksi *Bluetooth.*

Pada kesempatan ini pula, penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam pembuatan aplikasi ini khususnya kepada pembimbing Tugas Akhir dan teman-teman yang telah banyak membantu dalam pembuatan aplikasi dan penyusunan laporan ini.

Dalam kesempatan ini, penyusun mengucapkan terima kasih kepada:

1. Kedua orang tuaku yang selalu mendukungku dalam pengerjaan Tugas Akhir ini, dengan do'a, kepercayaan, kebanggaan, dukungan baik moril dan materil. Luv U Mama Papa...
2. Adik-adikku tersayang Wahyu Satria dan M. Iqbal yang telah mendukung, mengerti, dan selalu menghiburku dengan cinta dan do'a nya. Makasih bang udah rela ga pake handphone barunya demi kakakmu...
3. Seluruh keluargaku, nyai, wak-wak semua, serta sepupu-sepupuku tercinta yang telah perhatian dan mendukung penulis dengan do'a dan dalam segala hal,
4. Bapak Priyono Eko Sanyoto, selaku Direktur Politeknik Batam,
5. Bapak Agus Fatulloh, ST selaku pembimbing yang telah sabar, meluangkan banyak waktu dan tak henti-hentinya memberikan motivasi yang besar, bimbingan, dan arahan demi kelancaran Tugas Akhir ini,
6. Bapak Uuf Brajawidagda selaku Kaprodi Teknik Informatika.
7. Ibu Evaliata Sembiring selaku koordinator Tugas Akhir 1,
8. Bapak Ari Wibowo selaku koordinator Tugas Akhir 2 sekaligus Ketua Penguji Seminar yang memberikan arahan yang baik mengenai Tugas Akhir saya,
9. Bapak Afdhol Dzikri selaku Dosen Wali sekaligus Penguji Seminar dan Ibu Fida yang telah banyak memberikan kritik dan saran yang membangun mengenai keseluruhan dari Tugas Akhir saya,
10. Buat wak Ai, wak Miran, Kak Susi atas pinjaman handphonenya. Kak ica yang telah membantu mencarikan pinjaman handphone untuk Tugas Akhir ku,
11. Buat sahabat – sahabat ku tercinta, De2w, Fadhly, Ustadz sejuta akhwat alias Ijal, Trisno (eh.. Sutrisnawati) my buddy, Sri yang selalu menghayati, Andi Tonjang atas segala dukungannya, perjuangan kita ga sia-sia teman, U're the best pRendz..
12. Buat Ay yang selalu ada disaat suka dan duka selama ini, yang selalu mau mengerti (walaupun ni suka ngambek..), tempatku mencurahkan semuanya, tempat berbagi, selalu mendukung ku tak henti-hentinya, baik memberikan do'a, semangat, support, moril, serta materil. Makasih Ay, sukses ya. " Do the best Ay..! ",
13. Buat Senior-senior ku yang TeOPe BeGeTe deh, k'Hafizh Bari dan k'Aswin Triadhi yang sibuk tapi tetap mau sharing dan membagikan ilmunya kepada penulis demi kelancaran Tugas Akhir ini,
14. Kakak-kakak dan abang-abang di Bagian Umum Pemko Batam, tempat magang ku, pak firman, kak resa, kak lia, kak santy, umi, kak mona, kak epa, rini,pak agus bendri, bang man, bang bongki, bang ewin, bang koko, serta semuanya yang tidak

bisa penulis sebutkan satu-persatu atas dukungan do'a, motivasi serta keceriaan hari-hariku selama magang,

15. Teman-teman seasrama ku, kak uliz makasih atas pinjaman laptopnya, teman sekamar ku mbak epa dan lies, teman asrama sejatiku yayan dan ega, serta teman-teman seasrama lainnya atas do'a, pengertian dan dukungannya, "ka unee miss u all dek..!"
16. Teman-teman seperjuangan IF'06, Nadia Tamsil, Mega Budi Pratiwi, Yolan Profita Ningrum, Ranny Angraini, Gustiawati, Erlyza Mucharani, Herlina, Octo Giantama teman PA1 ku yang setia, Sapta Tirani teman PA2 ku yang rajin, dan buat semuanya yang tidak dapat disebutkan satu-persatu. Kalian semua telah banyak memberikan dukungan, semangat, nasihat, do'a, dan pelajaran bagiku.
17. Teman-teman seangkatan ku EL'06 dan AK'06, serta para junior ku.

Dalam pembuatan Tugas Akhir ini, penulis telah banyak mendapatkan pelajaran hidup yang sangat luar biasa dan berarti. Kesuksesan itu tidak akan dapat diraih tanpa niat yang kuat, usaha yang keras dan do'a yang tak henti, serta keyakinan bahwa kita bisa.

Penulis juga menyadari masih banyak kekurangan dan jauh dari kata sempurna dalam penyusunan buku Laporan Tugas Akhir ini dan pembuatan Aplikasi Otentikasi Koneksi *Bluetooth*. Oleh karena itu, segala saran dan kritik yang bersifat membangun sangat diharapkan untuk revisi dimasa yang akan datang. Semoga buku ini dapat bermanfaat bagi pembaca, khususnya bagi yang hendak mengembangkan aplikasi serupa.

Batam, 27 Juli 2009

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Bab 1 Pendahuluan

1.1 Latar Belakang

Dewasa ini keamanan sistem komunikasi menjadi tuntutan yang harus dipenuhi oleh pihak yang terlibat didalamnya, apalagi komunikasi digital yang sangat rentan terhadap tindakan penyadapan. Salah satu sistem komunikasi yang sampai saat ini masih terus ditingkatkan aspek keamanannya adalah komunikasi menggunakan media *Bluetooth*. *Bluetooth* merupakan media komunikasi lokal tanpa kabel (*local wireless communication*) yang semakin populer dewasa ini. Kepopuleran ini didorong oleh banyaknya v*endor* perangkat *mobile* yang menyertakan *Bluetooth* pada produk mereka sebagai salah satu fasilitas pengiriman data. Kemudahan dalam penggunaan mengakibatkan banyak pengguna menggunakan fasilitas ini.

Namun karena teknologi komunikasi *Bluetooth* yang bersifat *broadcast* (menyebar), sistem keamanan dalam pengiriman data melalui *Bluetooth* memiliki kelemahan yang dapat dimanfaatkan oleh pihak yang tidak berhak dalam melakukan tindakan penyusupan atau penyadapan. Kelemahan dari teknologi komunikasi *Bluetooth* ini terletak pada belum adanya otentikasi terhadap pengguna, proses otentikasi hanya dilakukan untuk perangkat, sehingga jika perangkat yang berkomunikasi sama maka dianggap proses komunikasi dilakukan dengan pengguna yang benar. Untuk itu dibuatlah suatu aplikasi yang mampu mengotentikasi pengguna guna memastikan koneksi dilakukan kepada pihak yang berhak.

1.2 Tujuan

Aplikasi ini dibuat bertujuan untuk :

1. Memberikan layanan keamanan koneksi *Bluetooth.*
2. Mengembangkan mekanisme otentikasi pengguna dalam mempertukarkan elemen-elemen pembentuk kunci privat, sehingga pihak yang tidak memiliki kunci privat tidak dapat terkoneksi.

1.3 Batasan Masalah

Adapun batasan masalah dalam aplikasi ini adalah :

1. Aplikasi ini hanya diinstal pada ponsel yang spesifikasinya mendukung Java MIDP 2.0 dan memiliki perangkat *Bluetooth.*
2. Aplikasi hanya bisa digunakan pada ponsel yang sudah terinstall aplikasi Otentikasi Koneksi *Bluetooth* yang akan menghasilkan nilai kunci privat sebagai pengotentikasi pengguna.
3. Aplikasi hanya digunakan untuk mengotentikasi pengguna saja.

1.4 Ikhtisar Buku

Laporan ini terdiri dari Bab Pendahuluan, Deskripsi Umum Aplikasi, Analisis, Deskripsi Perancangan , Implementasi dan Pengujian, Kesimpulan dan Saran serta Lampiran yang berhubungan dengan aplikasi yang dibuat.

Bab I Pendahuluan yang berisi penjelasan mengenai latar belakang pembuatan aplikasi, tujuan pembuatan aplikasi, batasan masalah pada aplikasi dan ikhtisar buku.

Bab II Deskripsi Umum Aplikasi yang berisi tentang deskripsi umum sistem yang memberikan gambaran mengenai aplikasi, karakteristik pengguna, batasan sistem, lingkungan operasional, serta aturan penamaan dan penomoran pada aplikasi.

Bab III Analisis yang berisi tentang dasar teori, skema jaringan, deskripsi fungsional yang mencakup konteks diagram pada aplikasi, dan analisis kebutuhan data yang berisi uraian aliran data yang dikelola oleh aplikasi.

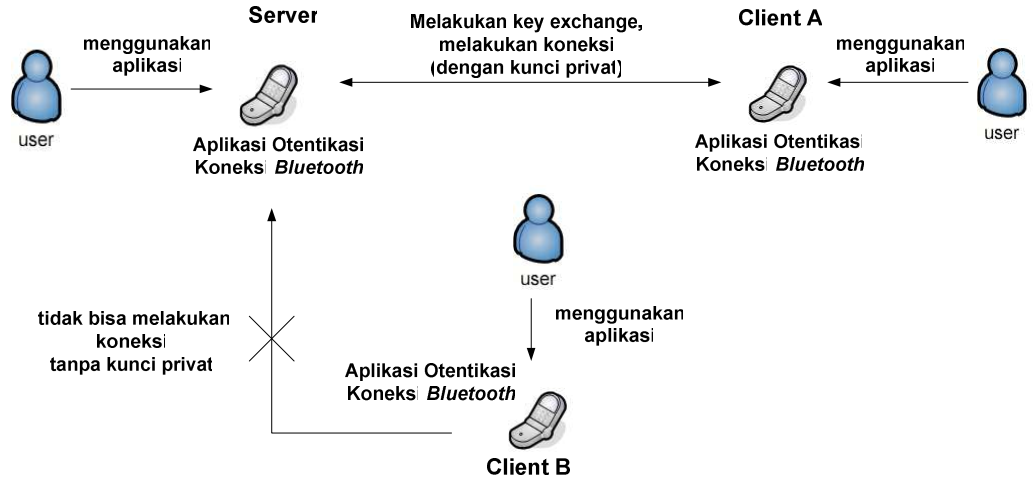
Bab IV Deskripsi Perancangan yang berisi tentang deskripsi data yang dikelola oleh aplikasi, koneksi jaringan, dekomposisi fungsional modul, spesifikasi kebergantungan antar layar, dan struktur menu.

Bab V Implementasi dan Pengujian yang berisi tentang spesifikasi kebergantungan antar modul, struktur direktori dan deskripsi file, serta pengujian dan hasilnya.

Bab VI Kesimpulan dan Saran yang berisi kesimpulan dari pencapaian tujuan aplikasi dan saran untuk pengembangan aplikasi di masa yang akan datang.

Bab 2 Deskripsi Umum Aplikasi

2.1 Deskripsi Umum Sistem



Gambar 2.1 Deskripsi Umum Sistem

Masing-masing pengguna mengaktifkan *Bluetooth* pada ponselnya lalu menggunakan aplikasi untuk berkomunikasi dengan ponsel lain. Pengguna sebagai Server adalah pengguna yang mengajak berkomunikasi dan yang lainnya sebagai Client. Server mencari perangkat *Bluetooth* yang aktif, setelah ditemukan server membuka koneksi untuk saling berkomunikasi dengan Client A kemudian melakukan proses pertukaran kunci (*key exchange*) untuk mendapatkan kunci privat yang selanjutnya akan disimpan dalam RMS (*Record Management System*) dan akan digunakan untuk berkoneksi kembali. Client A adalah client yang sudah pernah melakukan proses *key exchange* dan mendapatkan kunci privatnya, maka Client A dapat berkoneksi kembali dengan menggunakan kunci privatnya tersebut. Lain halnya dengan Client B yang tidak pernah melakukan proses *key* exchange, maka otomatis ia tidak memiliki kunci privat dan tidak bisa melakukan koneksi.

2.2 Karakteristik Pengguna

Tabel 2.1 Kategori Pengguna Aplikasi Otentikasi Koneksi *Bluetooth*

Kategori Pengguna	Tugas	Hak Akses ke aplikasi	Jabatan
User biasa	Melakukan koneksi via *Bluetooth*, melakukan pertukaran kunci (key exchange), melakukan komunikasi kembali	Penuh	User

2.3 Batasan

Batasan aplikasi Otentikasi Koneksi *Bluetooth* ini adalah :

1. Dalam pengembangannya aplikasi ini menggunakan Java 2 Microediton (J2ME)
2. Digunakan pada ponsel yang mendukung Java MIDP 2.0

2.4 Lingkungan Operasional

Aplikasi Otentikasi Koneksi *Bluetooth* mempunyai dua perangkat operasional yaitu perangkat keras dan perangkat lunak.

2.4.1 Perangkat Keras

Perangkat mobile yang mendukung J2ME (Java 2 Microedition) dengan spesifikasi :

a. Device Configuratin : CLDC-1.0 (Connected Limited Device Configuration)
b. Device Profile : MIDP-2.0 (Mobile Information Device Profile)
c. Memiliki perangkat *Bluetooth*

2.4.2 Perangkat Lunak

a. Perangkat keras
   - Prosesor : Pentium IV
   - Kebutuhan memori utama minimal : 256 MB
b. Operating system : Ms. Windows XP
c. Program/utilities lain : J2ME Wireless Toolkit 2.5.2 , Netbeans IDE 5.5.1

2.5 Aturan Penomoran

Aturan penamaan dan penomoran pada aplikasi ini sebagai berikut :

a. Bab diberi nomor diawali dengan Bab diikuti dengan nomor dan diikuti dengan judul atau nama bab tersebut.
   Misal: Bab 1. Pendahuluan
b. Sub bab diberi nomor diawali dengan nomor bab dan diikuti dengan nomor 1 dan seterusnya.
   Misal: 1.1. Latar Belakang
c. Sub-sub bab diberi nomor diawali dengan nomor sub bab dan diikuti dengan nomor 1 dan seterusnya.
   Misal: 2.4.1 Lingkungan Operasional
d. Tabel diberi nomor diawali dengan Tabel dan nomor bab dan diikuti dengan nomor 1 dan seterusnya.
   Misal: Tabel 2.1 (Tabel pertama pada Bab 2)
e. Penamaan gambar menggunakan nomor dan diikuti nama gambar.
   Misal: Gambar 2.1 Deskripsi Umum Sistem
f Fungsi diberi nomor diawali dengan huruf F dan diikuti dengan nomor 1 dan seterusnya.
   Misal: F1
g. File diberi nama sesuai dengan kode TA dan disertai dengan extention.
   Misal: IF-0809-B.04.doc
h. Layar diberi nama diawali dengan huruf L dan diikuti dengan nama menu.
   Misal: L_login (Layar pada menu login)
i. Penamaan lampiran : Lampiran<abjad>
   Misal : Lampiran A
j. Penamaan sub lampiran dimulai dari <abjad>”.”<angka> diikuti judul sub bab lampiran
   Misal : A.1 Spesifikasi

Bab 3 Analisis

3.1 Dasar Teori

Dalam konsep jaringan terdapat jaringan dengan kabel dan jaringan tanpa kabel (*wireless*). Jaringan dengan kabel biasanya dikenal dengan jaringan komputer. Jaringan komputer pada prinsipnya merupakan keterhubungan antara dua komputer atau lebih yang dapat saling berkomunikasi dan bekerja sama untuk tujuan tertentu. Jaringan komputer muncul dari adanya kebutuhan untuk berbagi data di antara para pengguna. Berdasarkan lokasi geografis dan ukurannya, jaringan terbagi ke dalam beberapa jenis, seperti LAN (Local Area Network), MAN(Metropolitan Area Network), dan WAN (Wide Area Network). Yang paling populer dari ketiga kategori jaringan ini adalah LAN (Local Area Network) karena LAN yang paling banyak digunakan, alasan LAN lebih banyak digunakan karena proses pengontrolan koneksi ke server yang relatif mudah, pertukaran informasi (sharing) yang juga lebih mudah, resiko kehilangan data dan tingkat keamanan yang lebih baik. Selain tiga jenis kategori jaringan di atas juga dikenal istilah internet (International Network) atau dapat definisikan sebuah jaringan raksasa. [WK09]

Teknologi yang memungkinkan komunikasi antara komputer satu dengan komputer lainnya tanpa menggunakan kabel (*wireless*) sehingga memungkinkan komputer kita dapat saling berkomunikasi dimananapun kita berada selama masih berada dalam range/ jarak dari pemancar frekuensi tersebut. Salah satu pengembangan dari konsep ini adalah jaringan *Bluetooth*. [WK09]

Bluetooth adalah suatu standard dan protokol komunikasi yang merancang untuk konsumsi tenaga rendah, dengan suatu cakupan pendek/singkat (power-class-dependent: 1 meter, 10 meter, 100 meter) yang didasarkan pada rendahnya transceiver microchip pada setiap alat. *Bluetooth* memungkinkan setiap alat untuk berkomunikasi dengan satu sama lain selama masih dalam satu cakupan. Alat *Bluetooth* menggunakan suatu sistem komunikasi radio, sehingga transmisi yang diterima cukup kuat. Adapun kelas-kelas dan jarak tempuh dari *Bluetooth* adalah :

Kelas Kecepatan Jarak tempuh
Kelas I : 100 mW (20 dBm) 100 meter
Kelas II : 2.5 mW (4 dBm) 10 meter
Kelas III: 1 mW (0 dBm) 1 meter

[WK09]

Bluetooth beroperasi dengan gelombang radio dengan frekuensi 2,4 Ghz ISM band pada 79 channel. *Bluetooth* memanfaatkan prinsip *frequency hopping spread* (FHSS) diantara 79 *channels* yang tersedia dengan kecepatan 1600 hops/second, yaitu setiap detik *Bluetooth* akan mengganti *channel* operasinya sebanyak 1600 kali. Hal ini ditujukan agar tidak terjadi bentrokan penggunaan saluran antara satu perangkat dengan perangkat lainnya. Dengan jarak komunikasi antara 10 sampai 100 meter dan hanya mengkonsumsi 2,5 mW daya dengan kecepatan frekuensi pengiriman data bias mencapai 3 Mbps. Hal ini jelas memperlihatkan bahwa *Bluetooth* adalah perangkat komunikasi yang murah daya dan murah biaya. [WK09]

Orang membutuhkan komunikasi untuk menjaga hubungan dengan temannya, peralatan dan layanan-layanan telepon lainnya. Di antara peralatan elektronik yang banyak orang miliki dan gunakan adalah telepon selular yang sering dibawa dimanapun mereka berada. Telepon Seluler atau Ponsel adalah salah satu alat komunikasi yang dapat dibawa kemana saja oleh pengggunanya. Dengan adanya perkembangan teknologi yang sangat pesat, ponsel saat ini tidak hanya digunakan untuk komunikasi suara, tetapi juga dapat membeli tiket, mencari berita, perbankan dan digunakan untuk berselancar di Internet, bahkan untuk mengoperasikan peralatan tertentu. [KW01]

Bluetooth pada ponsel merupakan teknologi yang telah lama muncul. Akan tetapi aplikasi-aplikasi yang memanfaatkannya belum banyak digali. *Bluetooth* pada ponsel bersifat terbuka dan ditujukan untuk komunikasi *wireless* untuk menghubungkan ponsel dengan headset atau peralatan lainnya seperti komputer. Spesifikasi *Bluetooth* mendifinisikan secara sistem lengkap dari level transmisi radio hingga lampiran aplikasi, termasuk *software stack.* Tetapi spesifikasi *Bluetooth* tidak menjelaskan bagaimana software API akan dikembangkan dan digunakan oleh software developers. Salah satu API yang dikembangkan adalah JABWT (Java API *Bluetooth Wireless* Technology) atau dinamai JSR-82. JABWT mendifinisikan API untuk pengembangan aplikasi-aplikasi berbasis *Bluetooth* menggunakan J2ME. [KW01]

Ponsel yang memiliki fasilitas JABWT di pasaran, antara lain Sendo X2, BenQ P30, BenQ P31, Motorola A1000, Sony Ericsson P910, Sony Ericsson P990i, Sony Ericsson K750, Sony Ericsson K800, Sony Ericsson W800, Sony Ericsson W810, Sony Ericsson W900, Sony Ericsson W850, Nokia 6681, Nokia 6682, Nokia 6680, Nokia 9500, Nokia 9300, Nokia 6600, Nokia 6620, Nokia 7610, Nokia 6630, Nokia 6260, Nokia 6280, Nokia 6670, Nokia 3230, Nokia 3250, Nokia 6230, Nokia 6255, Nokia 6300, Nokia N70, Nokia N80, Nokia N73, Nokia N95, Nokia N91, Nokia N90, Nokia N93, Siemens SK65, Siemens S65, Siemens S66, Siemens S6C, Siemens S6V, dan Panasonic X700. [KW01]

Kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena menjadi pokok dari fungsi komputer dan jaringan adalah data ataupun informasi. Komputer dan jaringannya menjadi sarana bagi distribusi data dan informasi, maka data dan informasi tersebut harus diamankan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. [MUN06]

Berdasarkan kunci yang digunakan, aplikasi ini menggunakan kriptografi kunci nirsimetris dimana terdapat sepasang kunci yaitu kunci publik dan kunci privat. Algoritma yang digunakan untuk pembentukan kunci publik dan kunci privat ini adalah Algoritma Diffie-Hellman. [MUN06]

Algoritma Diffie-Hellman diperkenalkan oleh Whitfield Diffie dan Martin E. Hellman pada tahun 1976. Algoritma Diffie-Hellman ini digunakan untuk mempertukarkan kunci antara pihak yang saling berkomunikasi. Algoritma ini bekerja pada saluran komunikasi publik yang tidak aman, namun dapat menghasilkan kunci (*shared secret key*) secara aman. Algoritma ini hanya sebatas untuk pertukaran kunci saja. [MUN06]

Secara sistematis Algoritma Diffie-Hellman digambarkan sebagai berikut :

Parameter Umum

Misalkan dua orang yang berkomunikasi adalah Alice dan Bob. Mula-mula Alice dan Bob menyepakati dua buah bilangan dasar **n** dan **g,** sedemikian sehingga g < n**.** Nilai n dan g tidak perlu rahasia, bahkan Alice dan Bob dapat membicarakannya melalui saluran yang tidak aman sekalipun.

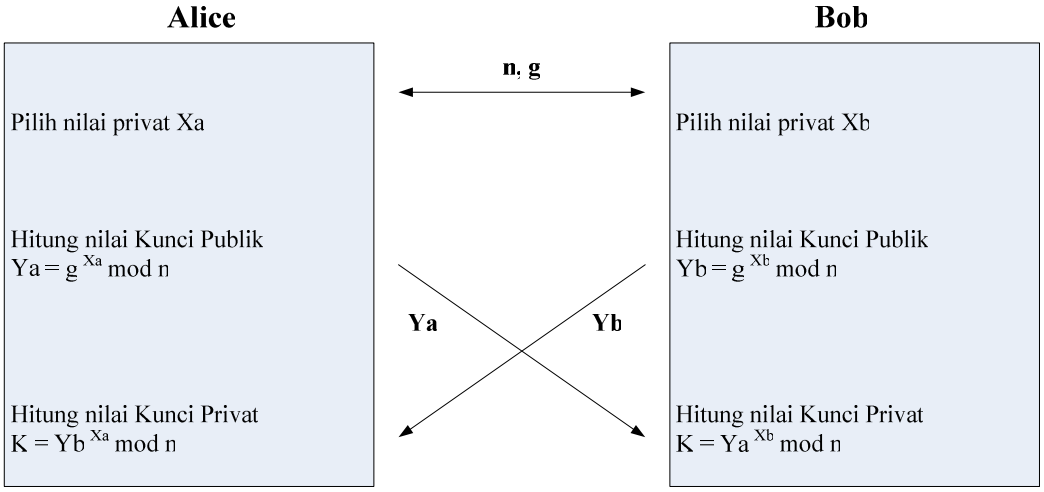
Algoritma Diffie-Hellman

1. Alice memilih nilai privat yang besarnya **Xa** dan mengirim kunci publik (**Ya**) dari hasil perhitungan berikut kepada Bob:
   $Ya = g^{Xa} \bmod n$
2. Bob memilih nilai privat yang besarnya **Xb** dan mengirim kunci publik (**Yb**) dari hasil perhitungan berikut kepada Alice:
   $Yb = g^{Xb} \bmod n$
3. Alice menghitung nilai kunci privat (**K**)
   $K = Yb^{Xa} \bmod n$
4. Bob menghitung nilai kunci privat (**K'**)
   $K' = Ya^{Xb} \bmod n$

Jika perhitungan dilakukan dengan benar, maka :

$K = K'$

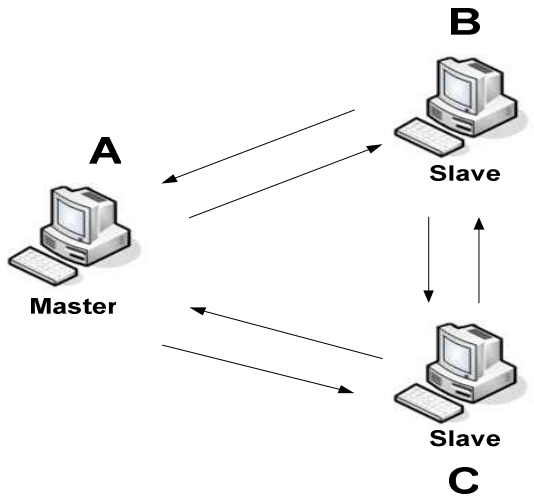
Di akhir perhitungan Alice dan Bob telah memiliki kunci privat yang sama, yaitu **K**.
[MUN06]



Gambar 3.1 Algoritma Diffie-Hellman

3.2 Skema Jaringan

Jaringan *Bluetooth* menggunakan prinsip master-slave. Perangkat yang bertindak sebagai master adalah perangkat yang menginisiasi terbentuknya koneksi. Komunikasi jaringan *Bluetooth* dikenal dengan nama point to point dimana ada satu master dan satu slave, selain itu *Bluetooth* juga memungkinkan dibentuknya jaringan yang terdiri dari lebih dari dua perangkat yang disebut piconet. Piconet merupakan bentuk lazim dari jaringan *Bluetooth* yang terbentuk dari sebuah master yang seterusnya akan disebut sebagai server dan lebih dari satu slave yang seterusnya akan disebut sebagai client.

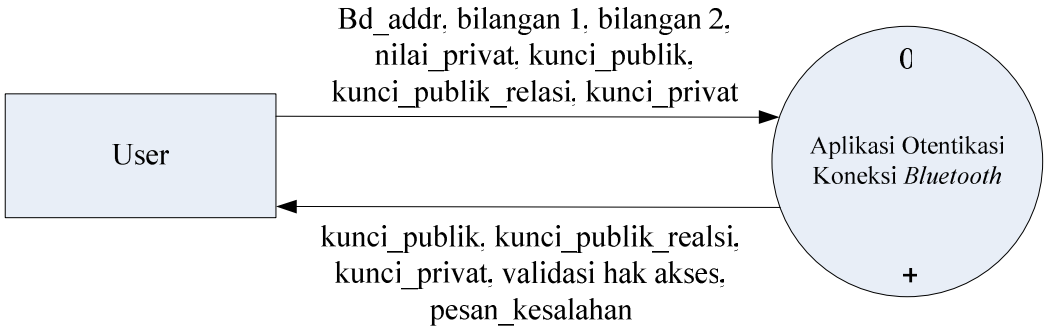


Gambar 3.2 Skema Jaringan

3.3 Deskripsi Fungsional

Deskripsi fungsional menjelaskan proses-proses yang dilakukan oleh aplikasi. Deskripsi fungsional terdiri dari context diagram, DFD level 1 dan DFD level 2. Context diagram merupakan gambaran aplikasi secara umum. Rincian fungsi dapat dilihat pada DFD level 1 dan DFD level 2

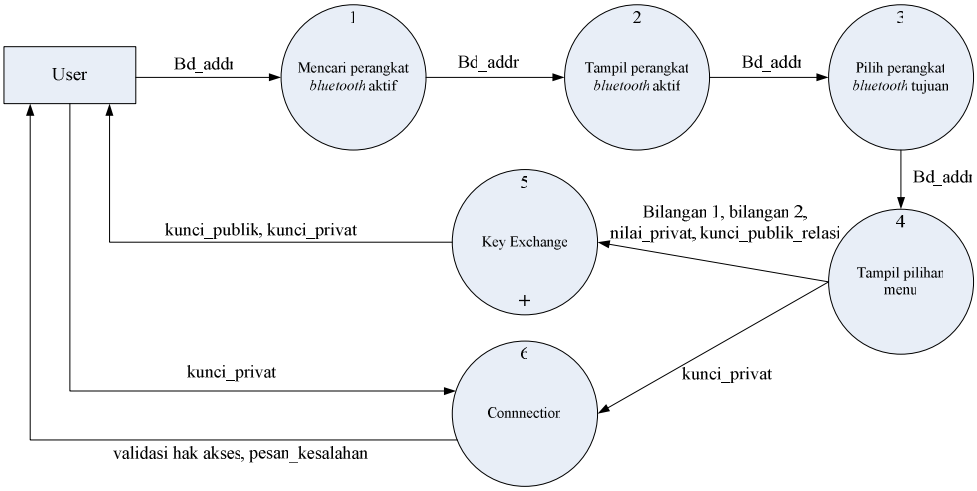
3.3.1 Context Diagram



Gambar 3.3 Context Diagram

User menjalankan aplikasi dengan menginput bilangan 1, bilangan 2, nilai_privat, kunci_publik, kunci_publik_relasi, kunci_privat, kemudian aplikasi akan mengelola inputan user, jika inputan benar maka user akan menerima output berupa kunci_publik, kunci_publik_relasi, kunci_privat, validasi_hak_akses pada perangkat yang diajak berkomunikasi. Akan tetapi jika inputan salah, maka aplikasi akan menampilkan pesan kesalahan bahwa user tersebut tidak berhak pada perangkat yang diajak berkomunikasi.

3.3.2 DFD Level 1

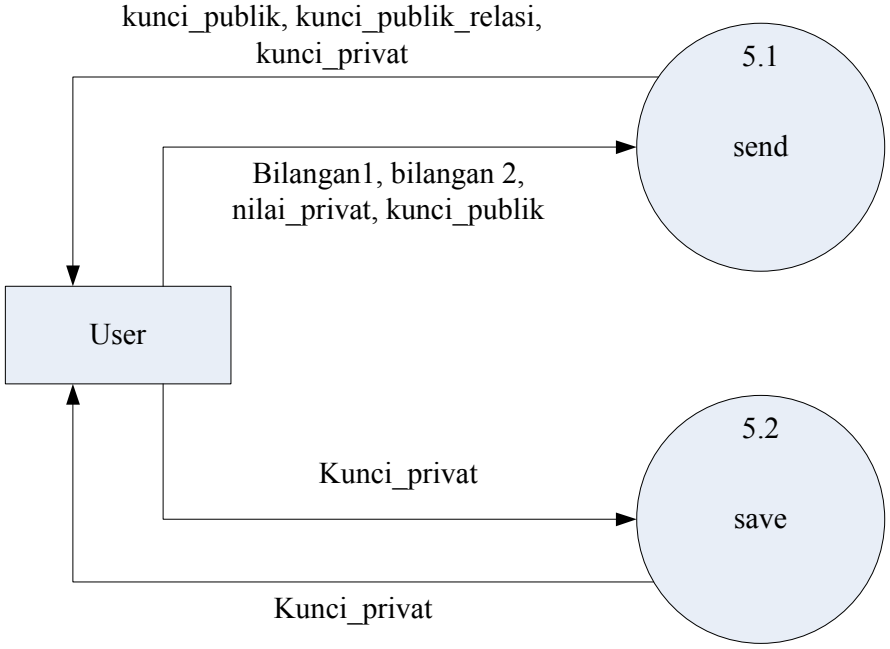


Gambar 3.4 DFD level 1

Diagram di atas menjelaskan proses-proses yang terjadi yaitu proses mengaktifkan perangkat *Bluetooth*, mencari perangkat *Bluetooth* aktif, tampil perangkat *Bluetooth* aktif, pilih perangkat *Bluetooth* tujuan, tampil pilihan menu yaitu *key exchange* dan *connection* yang akan di dekomposisi lagi menjadi proses berikutnya.

3.3.3 DFD Level 2

3.3.3.1 DFD Level 2 proses Key Exchange



Gambar 3.5 DFD level 2 Proses Key Exhange

Diagram di atas menjelaskan proses turunan dari proses Key Exchange yaitu proses Send dan Save, pada proses Send user (server) memasukkan inputan berupa bilangan 1, bilangan 2, nilai_privat, kunci_publik dan menghasilkan output berupa kunci_publik, kunci_publik_relasi, kunci privat dan nilai-nilai tersebut akan dikirimkan kepada client untuk dilakukan proses yang sama. Sedangkan pada proses Save user (server) menyimpan kunci_privat yang didapat dari proses Send, begitu juga pada client melakukan hal yang sama.

Bab 4 Deskripsi Perancangan

4.1 Deskripsi Data

Deskripsi Data menjelaskan data yang digunakan dalam aplikasi Otentikasi Koneksi *Bluetooth.* Terdapat enam macam data, yaitu :

Tabel 4.1 Deskripsi Data Aplikasi Otentikasi Koneksi *Bluetooth*

No	Nama Data	Tipe Data	Keterangan
1	Bilangan 1	Integer	Nilai bilangan acak yang merupakan elemen publik global
2	Bilangan 2	Integer	Nilai bilangan acak yang merupakan elemen publik global
3	Nilai Privat	Integer	Nilai bilangan privat dari masing-masing user
4	Kunci publik	Integer	Nilai kunci publik user (server dan client)
5	Kunci privat	Integer	Nilai kunci privat user (server dan client)
6	Hardware address	String	Alamat hardware *Bluetooth*

4.2 Koneksi Jaringan

Koneksi terjadi pada perangkat *Bluetooth* aktif, perangkat yang mengajak berkoneksi bertindak sebagai *master* (server) dan lainnya sebagai *slave* (client). Dalam pertukaran kunci server dengan menggunakan aplikasi mengirimkan data berupa bilangan 1, bilangan 2, dan kunci publik kepada client. Kemudian client menerima data tersebut untuk digunakan dalam aplikasi untuk membentuk kunci publik dan kunci privatnya, lalu kunci publiknya akan dikirimkan kembali kepada server guna membentuk kunci privat server.

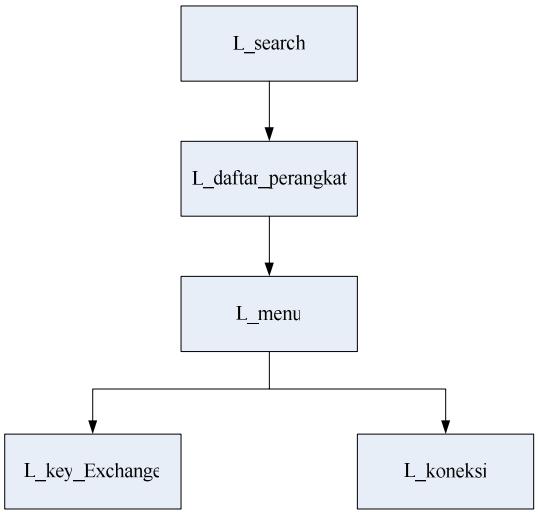
Dalam proses koneksi, client menggunakan kunci privatnya untuk berkoneksi dengan server untuk mengotentikasi pengguna, begitu juga dengan server.

4.3 Dekomposisi Fungsional Modul

Tabel. 4.2. Input-Proses-Output Aplikasi Otentikasi Koneksi *Bluetooth*

No	No. Fungsi	Fungsi/Proses	Tabel Input	Data Input	Tabel Output	Data output	Ket
1	F1	Search	-	-	-	-	
2	F2	key_exchange	-	Bilangan 1, bilangan 2, kunci_privat, kunci_publik _relasi	-	kunci_publik, kunci_privat	
3	F3	Koneksi	-	kunci_privat	-	-	

4.4 Spesifikasi Kebergantungan Antar Layar



Gambar 4.1 Spesifikasi Kebergantungan Antar Layar

4.5 Struktur Menu

Struktur menu Aplikasi Otentikasi Koneksi *Bluetooth* adalah sebagai berikut :

```
----- Search
----- Menu
       ---- Key Exchange
              ---- Send
              ---- Save
       ---- Connection
              ---- connect
```

Bab 5 Implementasi dan Pengujian

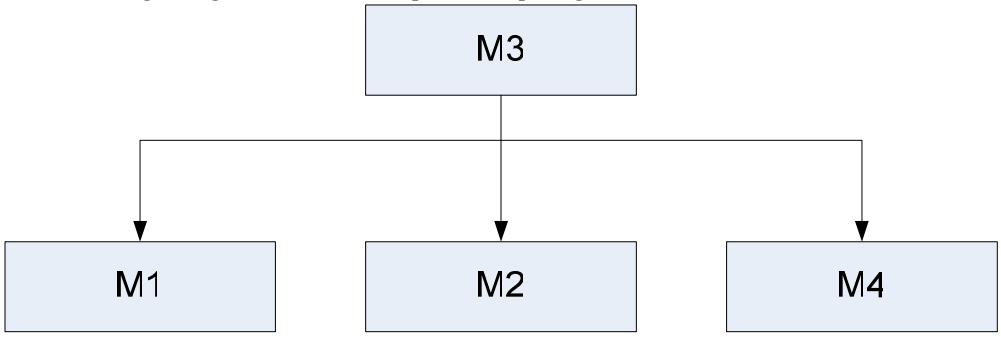
Setelah dilakukan tahap perancangan aplikasi, maka tahap selanjutnya adalah tahap Implementasi dan Pengujian. Tahap implementasi merupakan tahap dimana setiap fungsi yang telah dirancang sebelumnya diimplementasikan ke dalam bahasa pemrograman, yang dalam hal ini menggunakan bahasa JAVA2 for Mobile Edition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

5.1 Spesifikasi Kebergantungan Antar Modul

Spesifikasi Kebergantungan Antar Modul menjelaskan kebergantungan antar modul yang ada dalam aplikasi Otentikasi Koneksi *Bluetooth* :
Aplikasi Otentikasi Koneksi *Bluetooth* memiliki 3 modul yaitu :

4. Modul Connection (M1) adalah modul yang menangani koneksi *Bluetooth* dalam hal service pencarian perangkat *Bluetooth* server dan client.
5. Modul *keyExchange* (M2) adalah modul yang menangani pertukaran data-data bilangan yang akan digunakan dalam pembentukan kunci (kunci publik dan kunci privat).
6. Modul *MIDlet* (M3) adalah modul utama yang menjadi antar muka dan penghubung dari kelas-kelas yang ada.
7. Modul Koneksi Layer (M4) adalah modul yang menangani koneksi antara server dan client.

Spesifikasi Kebergantungan Antar Modul dapat dilihat pada gambar 5.1



Gambar 5.1 Spesifikasi Kebergantungan Antar Modul

5.2 Struktur Direktori dan Deskripsi File

Struktur Direktori dan Deskripsi File menjelaskan tentang struktur direktori dan pengumpulan fungsi menjadi file pada Aplikasi Otentikasi Koneksi *Bluetooth.*
Struktur direktori dan deskripsi file Aplikasi Otentikasi Koneksi *Bluetooth* dapat dilihat pada Tabel 5.1

Tabel 5.1. Daftar Direktori dan file Aplikasi Otentikasi Koneksi *Bluetooth*

Nama Direktori	Nama File	Nama Modul	Nama Fungsi	Keterangan
Project.bt	ClientForm.java	M2	keyExchange	Form client yang menangani fungsi keyExchange
	ServerForm.java	M2	keyExchange	Form client yang menangani fungsi keyExchange

Nama Direktori	Nama File	Nama Modul	Nama Fungsi	Keterangan
	SaveKey.java	M2	keyExchange	Fungsi untuk menangani penyimpanan kunci privat ke dalam RMS
	LogScreen.java	-	-	Form untuk menampilkan aktivitas *Bluetooth*
	ErrorScreen.java	-	-	Form yang menangani dan menampilkan kesalahan(Error/Exception)
	OtentikasiKoneksi*Bluetooth*.java	M3	koneksi	Kelas yang menjadi penghubung kelas-kelas yang lainnya
	Filter.java	M1	koneksi	fungsi untuk menyaring inputan kunci privat saat proses koneksi
	ServiceDiscoveryList.java	M1	search	Fungsi yang menangani koneksi *Bluetooth* server dan client
	SettingList.java	M1	search	Form pilihan server/client dan untuk memulai aplikasi
	TextScreen.java	-	-	Form yang menampung tampilan-tampilan dari fungsi-fungsi yang ada
	ConnectionForm.java	M1	koneksi	Form yang menangani koneksi pengguna dengan kunci privat
Project.bt.server	ServerConnectionHandler.java	M2	keyExchange	Kelas yang menangani fungsi-fungsi untuk key exchange pada server
	ServerConnectionHandlerListener.java	M2	keyExchange	Kelas yang menampung fungsi-fungsi untuk server
Project.bt.client	ClientConnectionHandler.java	M2	keyExchange	Kelas yang menangani fungsi-fungsi untuk key exchange pada client
	ClientConnectionHandlerListener.java	M2	keyExchange	Kelas yang menampung fungsi-fungsi untuk client
	ConnectionService.java	M2	keyExchange	Kelas yang menangani fungsi koneksi untuk client

5.3 Pengujian dan Hasilnya

Setelah dilakukan implementasi fungsi, maka selanjutnya adalah melakukan pengujian tehadap fungsi-fungsi seperti pada table 5.1
Rincian pengujian dan hasilnya dapat dilihat pada lampiran C : Dokumen Rinci Testing

Bab 6 Kesimpulan dan Saran

Setelah aplikasi Otentikasi Koneksi *Bluetooth* 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 Aplikasi Otentikasi Koneksi *Bluetooth* adalah
sebagai berikut:

1. Aplikasi sudah dapat memberikan layanan keamanan koneksi *Bluetooth*.
2. Aplikasi sudah dapat melakukan mekanisme otentikasi pengguna dalam mempertukarkan elemen-elemen pembentuk kunci privat, sehingga pihak yang tidak memiliki kunci privat tidak dapat terkoneksi.

6.2 Saran

Saran atas pengembangan Aplikasi Otentikasi Koneksi *Bluetooth* adalah sebagai berikut:

1. Aplikasi bisa melakukan sharing file dengan pihak yang otentik.
2. Aplikasi bisa berkoneksi dengan menggunakan grup.

DAFTAR PUSTAKA

[TO02] : Topley, Kim, "*J2ME in a Nutshell*", O'Reilly, 2002.

[SR08] : Shalahuddin, M & Rosa A.S, "*Pemrograman J2ME Belajar Cepat Pemrograman Perangkat Telekomunikasi Mobile*", Informatika, 2008.

[MUN06] : Munir, Rinaldi, "*Kriptografi*", Informatika, 2006.

[FN] : http://forum.nokia.com/

[JV] : http://java.sun.com/j2me

[JV2] : http://www.java2s.com/code/java/catalogJ2ME.htm

[KW01] : http://kuliahwireless.blogspot.com/2006/07/pengembangan-aplikasi-telepon-seluler.html

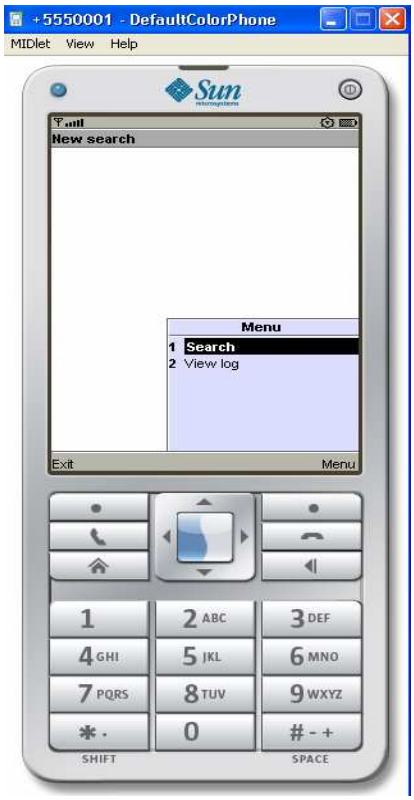
[WK09] : http://www.wikipedia.com

Lampiran A Perancangan Rinci Fungsional

A.1. Spesifikasi Fungsi/Proses Search<F1>

Identifikasi/Nama : Fungsi search
Deskripsi Isi : Mencari perangkat *Bluetooth* aktif
Jenis : Form

A.1.1. Spesifikasi Layar Utama



A.1.2. Spesifikasi Objek-Objek pada layar

Id_Objek	Jenis	Keterangan
cmdSearch	Command	Command untuk mencari perangkat *Bluetooth*
textScreen	TextScreen	Layar untuk menampilkan perangkat *Bluetooth* aktif

A.1.3. Spesifikasi layar pesan

No	Kasus	Pesan
1	Tidak ada perangkat *Bluetooth* yang aktif	No *Bluetooth* devices found

A.1.4. Spesifikasi proses/algoritma

A.1.4.1. <F1 > : fungsi search
Objek terkait : cmd_search
Event : on click
Berikut ini kerangkanya.

Initial State (IS): *Bluetooth* aktif dan command search belum di klik
Final State (FS): muncul textScreen perangkat *Bluetooth* aktif

Spesifikasi Proses/algoritma:
Klik command search
Mencari *Bluetooth* aktif
If *Bluetooth* aktif then
  TextScreen terisi daftar *Bluetooth* aktif
Else
  Tampil pesan “No *Bluetooth* Device Found”
End if

A.1.5. Spesifikasi Report

Tidak ada

A.2. Spesifikasi Fungsi/Proses Key Exchange<F2>

Identifikasi/Nama : Fungsi key_exchange
Deskripsi Isi : Mempertukarkan bilangan-bilangan untuk membentuk kunci publik dan kunci privat
Jenis : Form

A.2.1. Spesifikasi Layar Utama

A.2.2. Spesifikasi Objek-Objek pada layar

Id_Objek	Jenis	Keterangan
Str_addr	StringItem	Alamat *Bluetooth*
Str_connection	StringItem	Jumlah koneksi
Str_status	StringItem	Status koneksi
Tf_n1	TextScreen	Input bilangan 1
Tf_n2	TextScreen	Input bilangan 2
Tf_nPrivat	TextScreen	Input nilai privat
Tf_publicKey	TextScreen	Output kunci publik
Si_sPublicKey	StringItem	Output kunci publik server
Si_cPublicKey	StringItem	Output kunci publik client
Tf_privatKey	TextScreen	Output kunci privat
Calc1Command	Command	Klik untuk hitung kunci publik
Calc2Command	Command	Klik untuk hitung kunci privat
saveCommand	Command	Klik untuk menyimpan kunci privat
searchCommand	Command	Klik untuk mencari perangkat *Bluetooth* lain
sendCommand	Command	Klik untuk mengirim kunci publik ke perangkat *Bluetooth* tujuan
addConnectionCommand	Command	Klik untuk menambah koneksi dengan *Bluetooth* lain
logCommand	Command	Klik untuk melihat aktifitas *Bluetooth*
clearStatusCommand	Command	Klik untuk menghapus status

A.2.3. Spesifikasi layar pesan

No	Kasus	Pesan
1	Tf_n1 kosong	Bilangan 1 no argument
2	Tf_n2 kosong	Bilangan 2 no argument
3	Tf_nPrivat kosong	Nilai privat no argument
4	Tf_privatKey kosong	Kunci privat tidak boleh kosong

A.2.4. Spesifikasi proses/algoritma

A.2.3.1. <F2 > : fungsi key_exchange
Objek terkait : sendCommand, saveCommand
Event : on click
Berikut ini kerangkanya.

Initial State (IS): semua text field masih kosong

Final State (FS): kunci privat tersimpan

Spesifikasi Proses/algoritma:

```
(pada sisi server)
Masukkan bilangan 1 (tf_n1)
Masukkan bilangan 2 (tf_n2)
Masukkan nilai privat (tf_nPrivat)
Klik command create public key
Hitung nilai kunci publik(tf_publicKey)
    tf_publicKey = tf_n2 tf_nPrivat mod tf_n1
Tampil nilai kunci publik
Klik command send public key
Mengirim kunci publik ke perangkat Bluetooth tujuan
Kunci publik terkirim
Menunggu kiriman kunci publik dari perangkat Bluetooth tujuan
(pada sisi client melakukan hal yang sama)
Kunci publik telah diterima
Klik command create private key
Hitung kunci privat(tf_privatKey)
    tf_privatKey = si_sPublicKey tf_nPrivat mod tf_n1 (untuk client)
    tf_privatKey = si_cPublicKey tf_nPrivat mod tf_n1 (untuk server)
Tampil kunci privat
Klik command save key
If tf_privatKey kosong
    Tampil pesan "Kunci privat tidak boleh kosong"
Else
    Kunci privat tersimpan
    Tampil pesan "Kunci privat telah tersimpan"

End if

Klik command quit untuk keluar aplikasi
```

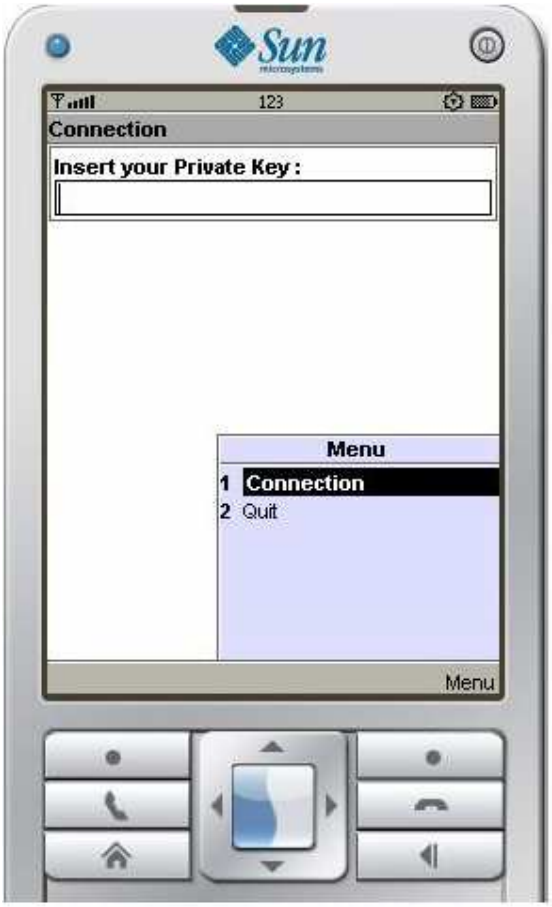
A.2.5. Spesifikasi Report

Tidak ada

A.3. Spesifikasi Fungsi/Proses Koneksi<F3>

Identifikasi/Nama : Fungsi koneksi
Deskripsi Isi : mengkoneksi perangkat *Bluetooth* dengan otentikasi
Jenis : Form

A.3.1. Spesifikasi Layar Utama



A.3.2. Spesifikasi Objek-Objek pada layar

Id_Objek	Jenis	Keterangan
Tf_privatKey	TextField	Input kunci privat
connectionCommand	Command	Klik untuk melakukan koneksi dengan otentikasi
quitCommand	Command	Klik untuk keluar dari aplikasi

A.3.3. Spesifikasi layar pesan

No	Kasus	Pesan
1	Kunci privat salah	Your Private Key not register…!
2	Kunci privat benar	Authenticated user...!!

A.3.4. Spesifikasi proses/algoritma

A.3.3.1. <F3 > : fungsi koneksi
Objek terkait : connectionCommand
Event : on click
Berikut ini kerangkanya.

Initial State (IS): semua text field masih kosong
Final State (FS): perangkat *Bluetooth* terkoneksi
Spesifikasi Proses/algoritma: Masukkan kunci privat Klik menu connection Buka koneksi untuk record store Baca record If kunci privat salah Tampil pesan “Your Private Key not register..!!” Else if Tampil pesan “Authenticated user..!!” End if Klik menu quit untuk keluar dari aplikasi

A.3.5. Spesifikasi Report

Tidak ada

Lampiran B DAFTAR RINCI FILE DAN DATA

B.1. Struktur direktori

B.1.1. Direktori pengembangan

Direktori Pengembangan adalah direktori yang berhubungan dengan tahap pengembangan Aplikasi Otentikasi Koneksi *Bluetooth*. Direktori Pengembangan terdiri atas dua subdirektori yaitu subdirektori Aplikasi dan subdirektori Dokumentasi.

- Aplikasi, berisi source code Aplikasi Otentikasi Koneksi *Bluetooth*
- Dokumentasi, berisi semua dokumen Aplikasi Otentikasi Koneksi *Bluetooth*

B.1.2. Direktori operasional

Direktori Operasional adalah direktori yang berhubungan dengan tahap implementasi aplikasi Otentikasi Koneksi *Bluetooth*. Direktori Operasional terdiri atas satu subdirektori yaitu subdirektori ExeFiles.

- ExeFiles, berisi file executable aplikasi Otentikasi Koneksi *Bluetooth* yang selanjutnya akan digunakan.

B.2. Isi Direktori Pengembangan

- Aplikasi, berisi source code aplikasi Otentikasi Koneksi *Bluetooth*
- Dokumentasi, berisi semua dokumen aplikasi Otentikasi Koneksi *Bluetooth*

B.2.1. Isi Subdirektori Pengembangan \Aplikasi

```
Volume in drive E is DATA
 Volume Serial Number is 08BC-6226

 Directory of E:\TA-B.04\Aplikasi\okb1

01/07/2009  07:20    <DIR>          .
01/07/2009  07:20    <DIR>          ..
17/03/2009  20:28             3.560 build.xml
01/07/2009  07:20    <DIR>          src
01/07/2009  07:20    <DIR>          nbproject
01/07/2009  07:20    <DIR>          dist
01/07/2009  07:20    <DIR>          build
               1 File(s)          3.560 bytes
               6 Dir(s)  36,331,982,848 bytes free
```

B.2.2. Isi Subdirektori Pengembangan \Dokumentasi

```
Volume in drive E is DATA
 Volume Serial Number is 08BC-6226

 Directory of E:\TA-B.04\Dokumentasi

07/22/2009  12:03 AM    <DIR>          .
07/22/2009  12:03 AM    <DIR>          ..
07/13/2009  11:43 AM            36,352 cover_laporan.doc
07/07/2009  02:31 PM           288,768 DeskripsiUmumSistem.vsd
07/07/2009  11:48 AM            94,720 dfd.vsd
07/22/2009  12:01 AM         1,422,848 IF-0809-B.04.doc
07/15/2009  02:47 PM           920,064 IF-0809-B.04.pps
07/15/2009  06:28 AM           913,408 IF-0809-B.04.ppt
07/15/2009  11:09 AM           280,576 lampiranA.doc
07/15/2009  11:10 AM            37,888 lampiranB.doc
07/15/2009  11:10 AM            36,864 lampiranC.doc
07/21/2009  11:59 PM            26,112 lampiranD.doc
07/21/2009  11:55 PM            29,184 lampiranE.doc
07/21/2009  11:56 PM            27,136 lampiranF.doc
              12 File(s)      4,113,920 bytes
               2 Dir(s)  36,331,982,848 bytes free
```

B.3. Isi Direktori Operasional

- ExeFiles, berisi file executable aplikasi Otentikasi Koneksi *Bluetooth* yang selanjutnya akan digunakan.

B.3.1. Isi Subdirektori Operasional\ ExeFiles

```
Volume in drive E is DATA
 Volume Serial Number is 08BC-6226

 Directory of E:\TA-B.04\Exe Files

07/22/2009  12:13 AM    <DIR>          .
07/22/2009  12:13 AM    <DIR>          ..
07/15/2009  10:30 AM               264 okb1.jad
07/15/2009  10:30 AM            45,020 okb1.jar
               2 File(s)         45,284 bytes
               2 Dir(s)  36,331,937,792 bytes free
```

B.4. File Instalasi

- ExeFiles, berisi file executable aplikasi Otentikasi Koneksi *Bluetooth* yang selanjutnya akan digunakan.

B.4.1. Isi File Instalasi

```
Volume in drive E is DATA
 Volume Serial Number is 08BC-6226

 Directory of E:\TA-B.04\Exe Files

07/22/2009  12:13 AM    <DIR>          .
07/22/2009  12:13 AM    <DIR>          ..
07/15/2009  10:30 AM               264 okb1.jad
07/15/2009  10:30 AM            45,020 okb1.jar
               2 File(s)         45,284 bytes
               2 Dir(s)  36,331,937,792 bytes free
```

Lampiran C Dokumen Rinci Testing

C.1. Tim penguji

1. Agus Fatulloh (AU)
2. Nadia Tamsil (NT)

C.2. Hasil Rinci Pengujian

No.	No.Fungsi	Deskripsi Fungsional	Kelompok Uji	Prosedur& Kasus uji	Hasil yang diharap	Hasil Test	Tester	Tgl Testing	Keterangan
1	F1	Proses mencari perangkat *Bluetooth* aktif	Normal	Mencari perangkat *Bluetooth* aktif	Device name ditemukan	Diterima	AU, NT	13 Juli 2009	
2	F2	Proses pembentukan dan pertukaran kunci public, dan elemen global lainnya	Normal	Membentuk Kunci publik, kunci privat dan mempertukarkan kunci publik dan elemen global	Kunci Publik terbentuk dan terkirim bersama elemen global, kunci privat terbentuk	Diterima	AU, NT	13 Juli 2009	

No.	No.Fungsi	Deskripsi Fungsional	Kelompok Uji	Prosedur& Kasus uji	Hasil yang diharap	Hasil Test	Tester	Tgl Testing	Keterangan
				lainnya					
			Normal	Menyimpan privat key	Muncul pesan "Privat Key telah tersimpan"	Diterima	AU, NT	13 Juli 2009	
			Data Salah	Field privat key kosong	Muncul pesan "Privat Key tidak boleh kosong"	Diterima	AU, NT	13 Juli 2009	
3	F3	Proses koneksi dengan perangkat *Bluetooth* aktif yang dipilih	Normal	Koneksi dengan perangkat *Bluetooth* aktif yang dipilih dengan memasukkan privat key	Bisa tekoneksi dengan baik	Diterima	AU, NT	13 Juli 2009	
			Data salah	Privat key tidak ada dalam RMS	Muncul pesan kesalahan "Your Private Key not register"	Diterima	AU, NT	13 Juli 2009	

Lampiran D Flow Map & Prosedur

Tidak ada

Lampiran E Logbook

Minggu	Periode	Ada/Tidak ada
2	8 September s/d 12 September 2008	Tidak ada
3	15 September s/d 19 September 2008	Ada
4	22 September s/d 24 September 2008	Ada
5	13 Oktober s/d 17 Oktober 2008	Ada
6	20 Oktober s/d 24 Oktober 2008	Ada
7	27 Oktober s/d 31 Oktober 2008	Ada
8	3 November s/d 7 November 2008	Ada
9	10 November s/d 14 November 2008	Tidak ada
10	17 November s/d 21 November 2008	Ada
11	24 November s/d 28 November 2008	Ada
12	1 Desember s/d 5 Desember 2008	Ada
13	9 Desember s/d 12 Desember 2008	Ada
14	15 Desember s/d 19 Desember 2008	Ada
15	22 Desember s/d 23 Desember 2008	Tidak ada
16	5 Januari s/d 9 Januari 2009	Tidak ada

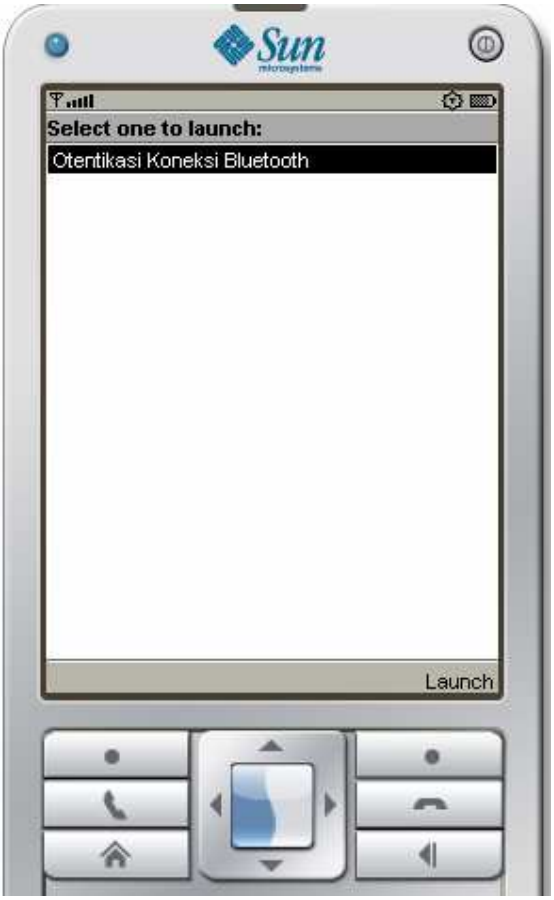
Lampiran F Manual Aplikasi

Aplikasi Otentikasi Koneksi *Bluetooth*

Sebelum melakukan proses instalasi pastikan ponsel anda memiliki *Bluetooth* dan mendukung J2ME dengan CLDC 1.0 dan MIDP 2.0.

Proses Instalasi

1. Instalasi ke Ponsel
   Hubungkan ponsel anda ke komputer. Untuk ponsel Nokia, anda dapat menggunakan kabel data atau *card reader* dan Nokia PC Suite sebagai software penghubung antara ponsel dan komputer.
   Copy-kan file “OtentikasiKoneksiBluetooth.jar” ke folder yang anda inginkan, pada sebagian ponsel juga meminta file .jad untuk di-copy ke ponsel.



Penggunaan Aplikasi

1. Sebelum anda menggunakan Aplikasi Otentikasi Koneksi *Bluetooth*, anda harus mengaktifkan *Bluetooth* yang ada di ponsel gar dapat melakukan koneksi.. Saat pertama menggunakan aplikasi, anda akan diminta memilih sebagai Server atau Client.

2. Terdapat pilihan menu :
   - **Start application,** untuk memulai aplikasi

Pada sisi **Server**, akan ada pilihan menu:

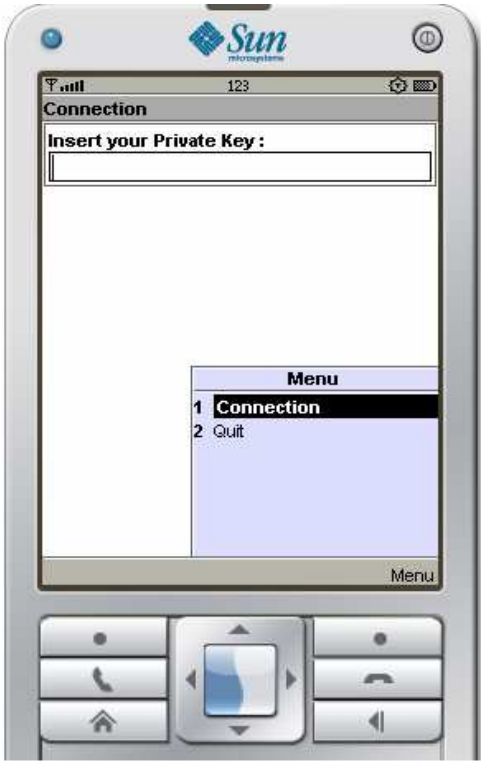
- **Search**, untuk mencari perangkat *Bluetooth* aktif
- **View log**, untuk melihat aktifitas *Bluetooth*
- **Help**, untuk panduan penggunaan aplikasi

Pada sisi **Client**, akan ada pilihan menu:

- **Connection**, untuk melakukan koneksi dengan menggunakan Private Key (Kunci Privat)
- **Key Exchange**, untuk melakukan pertukaran kunci untuk mendapatkan nilai Kunci Publik (Public Key) dan Kunci Privat (Private Key)

- **BT properties,** untuk melihat properties dari *Bluetooth*

3. Server melakukan proses pencarian perangkat *Bluetooth* yang aktif, sementara Client menunggu koneksi dari Server.
4. Masing-masing user (Server dan Client) dapat memilih menu utama, yaitu :
   - **Connection**, untuk melakukan koneksi dengan menggunakan Kunci Privat (Private Key). Private Key ini bisa didapat jika user sudah melakukan proses Key Exchange, jadi disarankan jika belum memiliki Private Key maka harus melakukan proses Key Exchange terlebih dahulu dengan memilik menu **Key Exhange**.



Secara sederhana proses yang dilakukan pada menu Connection ini adalah sebagai berikut :

1. Masukkan Kunci Privat (Private Key)
2. Pilih Menu Connection, jika Kunci Privat anda benar maka akan muncul pesan ” Authenticated User...!!”. Akan tetapi jika Kunci Privat anda salah maka akan muncul pesan "Error", "Your Private Key not register..!", segera lakukan proses Key Exchange.

- **Key Exhange,** untuk melakukan pertukaran kunci untuk mendapatkan melakukan pertukaran kunci untuk mendapatkan nilai Kunci Publik (Public Key) dan Kunci Privat (Private Key).

Secara sederhana proses yang dilakukan pada menu Key Exchange ini adalah sebagai berikut :

1. Masukkan bilangan sembarang pada Value 1 dan Value 2, Value2 < Value1
   (Nilai Value 1 dan Value 2 adalah sama antara Server dan Client)
2. Masukkan bilangan sembarang pada Private Value
   (Private Value adalah nilai yang rahasia dan tidak boleh diketahui oleh pihak lain untuk alasan keamanan)
3. Pilih menu Create Public Key untuk mendapatkan nilai Kunci Publik
4. Setelah Public Key didapat, pilih menu Send Public Key untuk mengirim kunci publik kepada relasi (Server/Client)
   (Menunggu kiriman Kunci Publik dari relasi (Server/Client))
5. Setelah Public Key dari relasi (Server/Client), maka pilih menu Create Private Key untuk mendapatkan nilai Kunci Privat .
6. Setelah Private Key didapat, maka pilih menu Save Key untuk menyimpan Kunci Privat anda.

Ada juga beberapa Menu lainnya, yaitu :

1. **Search for more**, untuk mencari perangkat *Bluetooth* aktif lainnya.
2. **Add connection**, untuk menambah koneksi dengan *Bluetooth* aktif lainnya.
3. **View log**, untuk melihat aktifitas dari *Bluetooth*.
4. **Clear Status**, untuk menghapus status.
5. **Help**, untuk petunjuk penggunaan aplikasi.