

BAB III

ANALISIS

Pada bab I telah dijelaskan bahwa pelaksanaan tugas akhir ini akan menghasilkan perangkat lunak aplikasi *SMS-Banking* dengan menggunakan algoritma RSA. Aplikasi ini merupakan aplikasi pada perangkat seluler untuk melakukan pembentukan tanda-tangan dan pada komputer pemroses untuk otentikasi tanda-tangan yang telah dibentuk. Aplikasi pada komputer tersebut akan terhubung dengan GSM *modem* sehingga dapat menerima SMS dari perangkat seluler yang berisi pesan transaksi dan tanda-tangan *digital*.

Bab ini akan membahas analisis terhadap perangkat lunak tersebut yang meliputi analisis umum sistem *real*, analisis aliran data, analisis perangkat lunak, dan analisis keamanan dan kelayakan tanda-tangan *digital* dengan menggunakan fungsi *hash* dan algoritma RSA.

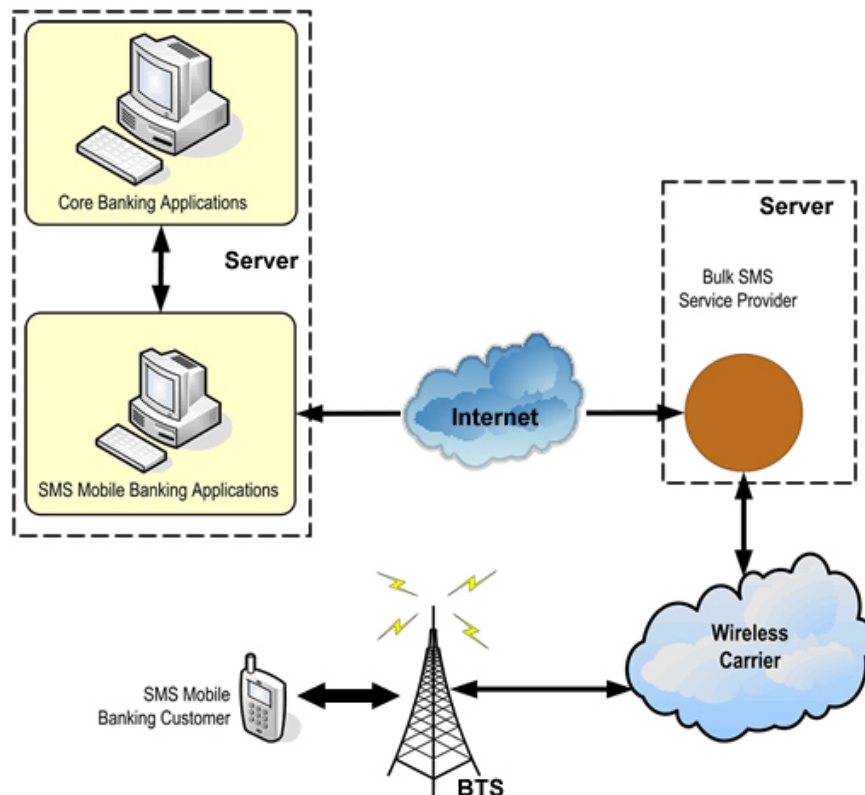
3.1 Analisis Umum Sistem

Aplikasi *SMS-Banking* ditujukan untuk mengirim data transaksi perbankan ke suatu *server* bank tertentu yang berbasis SMS (*Short Message Service*). SMS- Banking merupakan sebuah aplikasi yang menjawab kebutuhan akan pelanggan bank untuk dapat melakukan transaksi perbankan kapanpun dan dimanapun. Untuk itu, bank menyediakan informasi detail mengenai *account* pelanggan dan kemampuan transaksi *real-time* hanya dengan menggunakan perangkat seluler mereka yaitu dengan menggunakan layanan SMS. *SMS-Banking* menyediakan layanan yang dapat digunakan oleh penggunanya secara langsung meliputi :

1. Mendapatkan informasi mengenai saldo pelanggan
2. Mendapatkan informasi mengenai tiga transaksi terakhir
3. Melakukan transfer *account* ke rekening pengguna yang lain
4. Membayar tagihan kartu kredit
5. Mendapatkan informasi mengenai kurs valuta asing

6. Melakukan transaksi ubah nomor PIN

Untuk menunjang layanan tersebut, diperlukan sebuah gambaran sistem secara umum mengenai bagaimana proses *SMS-Banking* ini dilakukan dan menghasilkan keluaran yang sesuai dengan keinginan dari bank dan pelanggan. Gambaran mengenai arsitektur *SMS-Banking* terdapat pada Gambar III-1.



Gambar III-1 Arsitektur SMS-Banking [SAC05]

Dalam melakukan transaksi *SMS-Banking* yang sebenarnya, pelanggan akan mengirimkan sebuah pesan SMS yang berisi sebuah struktur kode tertentu kepada penyedia nomor layanan perbankan tertentu (*Bulk SMS Service Provider*). Nomor layanan yang disediakan oleh *service provider* biasanya berupa nomor pendek yang terdiri dari 4 angka seperti 9386, 8888, 4343, dan sebagainya. Penyedia layanan nomor ini selanjutnya akan meneruskan pesan yang diterimanya ke aplikasi *SMS-Banking* yang ada di bank. Aplikasi *SMS-Banking* yang ada di bank terhubung dengan komputer *server* (*Core Banking Server*) yang menyimpan informasi mengenai rekening bank pelanggan sekaligus melayani permintaan (*request*) dari pelanggan. Hasil permintaan dari pelanggan akan dikirimkan oleh aplikasi *SMS-Banking* ke *Bulk*

SMS Service Provider dan dilanjutkan ke nomor telepon seluler pelanggan melalui layanan SMS.

Bank secara proaktif mengirimkan data kepada pelanggan ketika merespon suatu transaksi. Sebagai contoh, transfer *account* dari rekening satu ke rekening yang lain. Data akan dikirimkan ke pelanggan dalam dua metode [SAC05]:

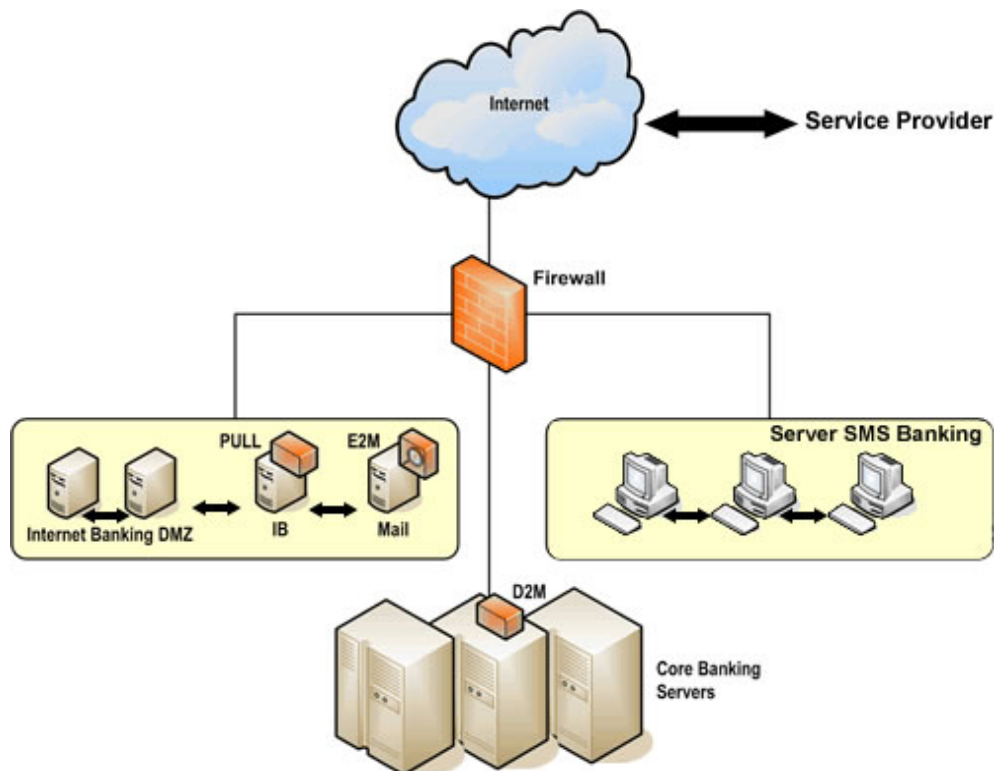
- a. *E-mail to mobile* (E2M), bank mengirimkan sebuah email ke aplikasi *SMS-Banking* yang terdapat di bank melalui alamat email yang spesifik. Email ini akan mengandung isi pesan tertentu beserta dengan nomor perangkat seluler pelanggan. Aplikasi *SMS-Banking* yang terdapat di bank mengirimkan pesan dalam format tertentu (sebagai contoh, tag XML yang merupakan bagian dari *string* pesan *query* HTTP GET) ke *server* aplikasi *service provider*. Dari sini, informasi dari tag XML akan di *extracted* dan dikirimkan sebagai SMS ke nomor telepon seluler pelanggan.
- b. *Database to mobile* (D2M), aplikasi *SMS-Banking* yang terdapat di bank akan secara aktif melakukan *polling* ke basis data *server* bank. Sebagai contoh, ketika transaksi pemindahan *account* dari satu rekening ke rekening yang lain, aplikasi mengirimkan pesan tertentu ke aplikasi *server* yang disediakan oleh *service provider*. Format pesan mungkin bisa sama dengan format pada E2M. Pesan ini kemudian dikirimkan sebagai SMS ke nomor telepon seluler pelanggan.

Berdasarkan kedua metode di atas, implementasi tanda-tangan digital SMS untuk *SMS-Banking* akan menggunakan metode D2M. Kelebihan metode ini diantaranya :

1. Proses respon yang diberikan lebih cepat. Hal ini dikarenakan aplikasi langsung berhubungan dengan basis data *server*, tanpa melalui *mail server* terlebih dahulu. Selain itu, protokol komunikasi yang digunakan lebih efektif karena sesuai dengan kebutuhan.
2. Format data yang digunakan lebih dapat disesuaikan dengan kebutuhan tanpa harus melakukan *parsing* lebih seperti pada *parsing* pesan *e-mail*. *Parsing e-mail* dilakukan dengan memisahkan bagian-bagian yang ada seperti *header* (*summary*, *sender*, *receiver*, dan informasi lain) dan *body(text)*. Padahal yang akan digunakan hanya pada bagian *body* saja. Hal ini mengakibatkan ada proses *parsing* tambahan pada *header* dan *body e-mail* untuk mendapatkan

data transaksi. Sedangkan dengan metode D2M, *parsing* dapat langsung dilakukan tanpa harus memisahkan bagian *header* dan *body* karena hanya terdiri dari *body*.

3. Tingkat keamanan dari data yang dipertukarkan lebih aman. Keamanan ini didapatkan karena format data yang dikirimkan hanya diketahui oleh pihak bank. Selain itu proses transaksi yang terjadi hanya terjadi pada jaringan internal bank (LAN). Gambaran mengenai jaringan LAN perbankan untuk *SMS-Banking* terdapat pada Gambar III-2.



Gambar III-2 Komponen infrastruktur *SMS-Banking* [SAC05]

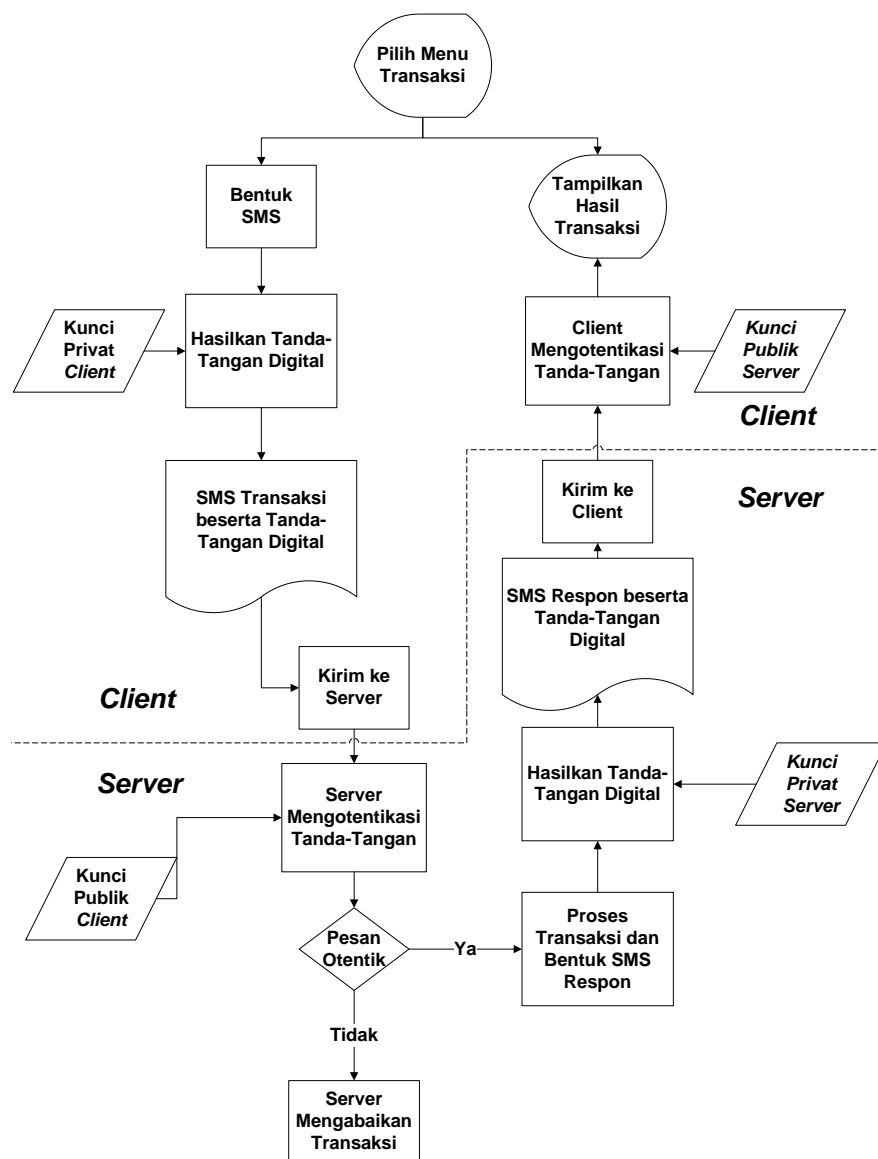
Adapun kelemahan dari pemilihan metode D2M ini adalah sebagai berikut :

1. Sistem arsitektur *SMS-Banking* kurang dapat terintegrasi dengan baik dengan fasilitas *e-banking* dari bank yang bersangkutan. Hal ini diakibatkan transaksi melalui *e-banking* kerap menggunakan *e-mail* sebagai protokol komunikasi antara aplikasi server dengan basis data bank.

- Pengaksesan basis data secara langsung memerlukan otentikasi format *query* yang tepat. Hal ini dimaksudkan agar tidak terjadi kesalahan ketika *entry* sebuah *query*.

3.2 Analisis Aliran Data SMS-Banking

Pada analisis sebelumnya telah dijelaskan mengenai bagan secara umum dan keterhubungan antar komponen yang terdapat pada *SMS-Banking*. Gambar III-3 akan menunjukkan diagram alir dari *SMS-Banking*.



Gambar III-3 Diagram aliran data SMS-Banking

Untuk lebih memperjelas bagaimana sebenarnya aliran data yang terjadi dalam *SMS-Banking* akan dijelaskan sebagai berikut :

1. Pelanggan menggunakan aplikasi *SMS-Banking* yang terdapat pada telepon selulernya untuk melakukan transaksi perbankan. Dalam penggunaannya, pelanggan akan memilih menu transaksi perbankan kemudian aplikasi tersebut akan mengubah menu yang dipilih menjadi sebuah bentuk kode tertentu dan mengirimkannya ke dalam bentuk SMS.
2. Sebelum SMS dikirimkan, kode yang terbentuk tersebut akan diberi tanda-tangan *digital* untuk menjamin keamanan pengirimannya ke komputer *server* yang disediakan oleh *service provider (Bulk SMS Service Provider)*. Pemberian tanda-tangan *digital* ini melibatkan kunci-publik dan kunci rahasia yang digunakan untuk membentuk tanda-tangan *digital*. Untuk beberapa transaksi yang mempunyai isi pesan yang penting, seperti ganti nomor pin, bagian pesan transaksi SMS akan dienkripsi terlebih dahulu dengan menggunakan kriptografi kunci simetri.
3. SMS yang dikirimkan dari perangkat seluler pelanggan akan diterima oleh *Bulk SMS Service Provider* dalam hal ini adalah komputer *server* yang dimiliki oleh penyedia layanan nomor tertentu. SMS yang masuk diterima melalui perangkat *GSM modem* yang terhubung dengan komputer tersebut. SMS yang diterima oleh *GSM modem* tersebut masih mengandung tanda-tangan digital. Komputer lalu akan memeriksa apakah nomor telepon pelanggan dikenali atau tidak. Jika tidak dikenali, maka SMS tidak akan diteruskan pada aplikasi *SMS-Banking* yang terdapat di bank. Setelah dikenali, komputer akan memeriksa apakah format SMS yang diterima telah sesuai dengan format yang ditentukan.
4. Jika SMS memang berasal dari pelanggan yang terdaftar layanan ini dan format SMS telah benar, maka SMS akan diteruskan ke aplikasi *SMS-Banking* yang terdapat di bank. Selanjutnya, aplikasi tersebut akan melakukan verifikasi terhadap data SMS yang diterima untuk memeriksa keabsahannya. Pemeriksaan keabsahan ini berdasarkan tanda-tangan *digital* yang diberikan pada SMS tersebut dengan melibatkan kunci-publik dan kunci privat yang digunakan pada saat pembentukan tanda-tangan *digital*. Kunci yang digunakan pada saat verifikasi merupakan pasangan kunci yang digunakan pada saat pembentukan tanda-tangan

digital. Untuk itu, pada komputer ini perlu disimpan tabel (Tabel III-1) pemetaan kunci-publik dari pasangan nilai e dan n .

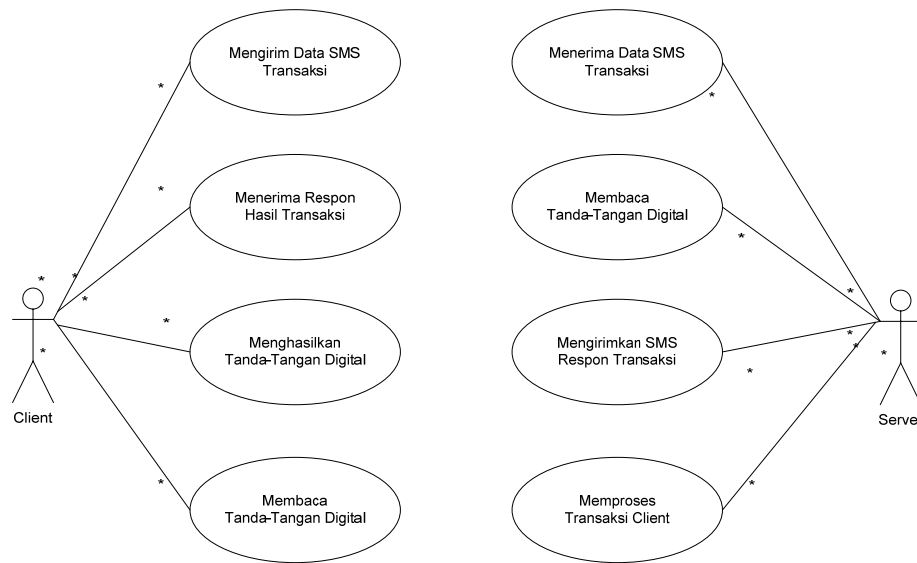
Tabel III-1 Pemetaan Kunci-Publik dan Kunci-Privat

No Telp	No Rekening	$n1$	e	$n2$	d
+6285220842578	112-121-2341	3337	79	3233	17
+6285220075338	152-128-2643	3233	17	1241	87
+6208165422077	132-127-2341	1311	19	3337	79
+6208562245781	116-121-2547	1241	87	1311	19
...
..

5. Jika hasil verifikasi positif, maka disusun *query* untuk transaksi perbankan yang berasal dari pesan SMS tersebut. Setelah itu, *query* akan dikirim ke *server* basis data yang terdapat di bank untuk diproses. Kemudian basis data akan diupdate berdasarkan *query* tersebut.
6. Jika hasil verifikasi negatif, maka data transaksi perbankan yang terdapat pada pesan SMS tersebut diabaikan. Hasil verifikasi negatif ini diakibatkan oleh adanya perubahan pada data SMS sehingga pada saat verifikasi tanda-tangan *digital* yang diperoleh berbeda dengan tanda-tangan *digital* yang diberikan pada awalnya.
7. Hasil verifikasi yang positif akan memicu *server* untuk membentuk SMS hasil *request* dan mengirimkan ke *client* sehingga pengguna dapat melihat dan mengetahui hasil transaksi yang diminta. Setiap SMS yang dikirimkan oleh *server* akan dibubuhkan tanda-tangan *digital* dengan menggunakan kunci publik dari *client*. Proses pertukaran kunci publik dan kunci privat akan dibahas pada subbab selanjutnya.

3.3 Analisis Perangkat Lunak Simulasi *SMS-Banking*

Analisis perangkat lunak untuk mengimplementasikan simulasi sistem *SMS-Banking* akan membahas mengenai spesifikasi pembagian perangkat lunak, spesifikasi kebutuhan perangkat lunak, dan batasan sistem. Gambar mengenai *use case* hasil analisis terdapat pada Gambar III-4.



Gambar III-4 Use Case *Client-Server SMS-Banking*

3.3.1 Spesifikasi Pembagian Perangkat Lunak

Perangkat lunak ini akan dibagi menjadi dua bagian utama, yaitu

1. *Client*

Pada bagian ini aplikasi yang akan dibangun merupakan aplikasi yang dapat berjalan di atas telepon seluler pengguna. Untuk memfasilitasi pengembangan tersebut, maka akan digunakan teknologi J2ME yang mendukung pembangunan aplikasi SMS. Sedangkan untuk melakukan pemberian tanda-tangan pada pesan SMS, maka akan digunakan *library Bounce Castle Crypto* yang menyediakan fitur *hashing* dan operasi *big integer* pada telepon seluler.

2. *Server*

Pada bagian ini sistem akan dibagi kembali menjadi 2 bagian yaitu penerima SMS dan pemroses transaksi. Untuk penerima SMS, pekerjaan yang akan dilakukan adalah menerima SMS, memeriksa apakah nomor telepon terdaftar, serta memeriksa apakah format SMS telah benar. Sedangkan untuk pemroses transaksi terdiri dari : pengecekan keabsahan tanda-tangan *digital* dan pemrosesan transaksi perbankan. Pada bagian ini juga akan diimplementasikan skema basis data yang dibutuhkan untuk pemrosesan *query* transaksi perbankan.

3.3.2 Spesifikasi Kebutuhan Perangkat Lunak *Client*

Spesifikasi kebutuhan perangkat lunak *client* secara umum terdiri dari :

- i. Mengirimkan data SMS yang berisi transaksi perbankan

Data SMS perbankan, berisi nomor rekening pelanggan dan transaksi, harus dapat sampai ke *server* pusat sehingga proses *update* basis data dapat dilakukan. Pada sistem *SMS-Banking* ini data transaksi tidak dikirimkan langsung ke *server* pusat bank tetapi melalui *SMS Bulk Service Provider* yang disediakan oleh penyedia layanan nomor pendek tertentu. Data SMS yang dikirimkan harus sesuai dengan protokol komunikasi SMS pada umumnya.

- ii. Membentuk format data SMS yang terdefinisi

Format data SMS yang dikirim harus sesuai dan terdefinisi oleh komputer di sisi *server*. Oleh karena itu, perlu adanya penetapan format data SMS yang nantinya akan diberi tanda-tangan *digital*. Format data SMS tersebut meliputi urutan *string* nomor rekening sampai dengan transaksi yang akan dilakukan dan separator antara keduanya. Secara umum, format data SMS untuk transaksi *SMS-Banking* adalah sebagai berikut :

<Nomor-Seri> <No-Rekening> <Transaksi> <Atribut-Transaksi-1> ... <Atribut-Transaksi-N>

Setiap transaksi memiliki n atribut ($0..n$) yang berbeda-beda tergantung pada jenis transaksi. Di dalam format tersebut terdapat nomor seri yang dimaksudkan untuk keamanan data yaitu pihak ketiga tidak akan bisa mengirimkan transaksi yang sama secara berulang yang telah dilakukan oleh pelanggan sebenarnya. Data SMS transaksi tersebut akan berbentuk sebagai berikut :

1. Format data SMS transaksi ubah nomor PIN

<Nomor-Seri> <No-Rekening> <Ubah-PIN> <No-PIN-lama> <No-PIN-baru>

Contoh : a54c23d 0028410018 UBAH-PIN 5432 3219

2. Format data SMS transaksi transfer *account* ke rekening lain

<Nomor-Seri> <No-Rekening> <Transfer> <No-Rekening-lain> <Jumlah transfer>

Contoh : a54c93d 0028410018 TRANSFER 0028510713 1000000

3. Format data SMS transaksi cek saldo

<Nomor-Seri> <No-Rekening> <Cek-Saldo>

Contoh : a54c43d 0028410018 CEK-SALDO

4. Format data SMS transaksi info valuta asing

<Nomor-Seri> <No-Rekening> <Valas> <Nama-MataUang >

Contoh : a54c43d 0028410018 VALAS US\$

5. Format data SMS transaksi pembayaran tagihan kartu kredit

<Nomor-Seri> <No-Rekening> <Tagihan> <Jenis-Tagihan>

Contoh : a54c43d 0028410018 TAGIHAN KARTU-KREDIT

6. Format data SMS transaksi info tiga transaksi terakhir

<Nomor-Seri> <No-Rekening> <Info-Transaksi>

Contoh : a54c43d 0028410018 INFO-TRANSAKSI

iii. Keamanan data pengiriman dengan pemberian tanda-tangan digital

Data SMS yang dikirimkan dan diterima oleh komputer *server* harus merupakan data SMS transaksi asli yang berasal dari pelanggan bank tertentu tanpa perubahan apapun. Untuk menjamin hal tersebut, maka aplikasi harus dapat memberikan tanda-tangan *digital* pada data transaksi SMS. Untuk dapat memberikan tanda-tangan *digital*, maka perangkat *client* harus mendukung operasi *big integer* dan pengoperasian bit-bit pesan SMS. Selain itu, perangkat *client* harus mampu melakukan enkripsi pesan SMS yang berisi pesan yang penting dan harus dirahasiakan.

iv. Mengenkripsi bagian pesan tertentu yang bersifat rahasia

Pesan transaksi yang akan dikirimkan harus dikategorikan terlebih dahulu menurut jenis transaksinya. Untuk transaksi yang melibatkan nilai nominal

uang atau nomor PIN harus dilakukan enkripsi terlebih dahulu terhadap nilai-nilai tersebut. Misalnya jika terdapat transaksi perubahan nomor PIN, maka nomor PIN semula dan nomor PIN yang baru harus dikirimkan dalam keadaan terenkripsi dengan menggunakan kunci simetri (DES) yang dimiliki oleh pengguna. Transaksi-transaksi yang harus dienkripsi terlebih dahulu pada bagian tertentu selain perubahan nomor PIN adalah transaksi transfer uang ke nomor rekening yang lain.

- v. Pengidentifikasian SMS response yang diterima, hasil dari request ke bank

SMS yang diterima oleh *client* yang merupakan hasil *request* transaksi dari pelanggan harus dapat diidentifikasi sehingga pelanggan dapat mengetahui apakah transaksi yang dilakukannya dapat diproses dan berhasil atau tidak. Data SMS yang diterima ini memiliki format sebagai berikut :

<No-Rekening> <Nama-Transaksi> <Waktu> <Berhasil/Gagal> <Hasil Transaksi>

Contoh : 0028410018 CEK-SALDO 17072007-13:40 BERHASIL 31500000

Untuk menjamin bahwa SMS yang diterima tidak mengalami perubahan dan memang berasal dari pihak bank, maka data SMS tersebut juga akan dilengkapi dengan tanda-tangan *digital*. Dengan kata lain, aplikasi akan memiliki 2 buah kunci yang tidak sepasang, yaitu kunci privat untuk tanda-tangan *digital* data SMS yang akan dikirimkan, sedangkan kunci-publik untuk tanda-tangan *digital* data SMS yang diterima dari bank.

3.3.3 Spesifikasi Kebutuhan Perangkat Lunak Server

Spesifikasi kebutuhan perangkat lunak pada sisi *server* untuk *Bulk SMS Service*

Provider secara umum terdiri dari :

- i. Menerima SMS yang berasal dari pelanggan

Perangkat lunak *Bulk SMS Service Provider* harus mampu menerima SMS yang berasal dari pelanggan. Untuk melakukan hal ini, diperlukan perangkat GSM *modem* yang dapat menerima SMS yang masuk secara utuh. Dikarenakan menggunakan perangkat GSM *modem*, maka perangkat lunak harus dapat mengenali *AT Command* (perintah-perintah GSM, seperti membaca SMS, mengirimkan SMS, dan sebagainya).

- ii. Memeriksa apakah nomor pelanggan terdaftar untuk melakukan transaksi

Setelah SMS yang diterima melalui GSM *modem*, maka komputer akan memeriksa apakah nomor telepon dari SMS yang masuk terdaftar dalam basis data pengguna layanan *SMS-Banking* atau tidak. Jika memang tidak terdaftar, maka komputer tidak perlu melakukan proses selanjutnya terhadap data SMS tersebut.
- iii. Memeriksa apakah format data transaksi sudah benar

Perangkat lunak mampu memeriksa apakah format SMS yang diterima sudah sesuai dengan aturan yang sudah didefinisikan sebelumnya. Hal ini ditujukan agar pihak bank dapat langsung mengambil tanda-tangan *digital* dan mengubah data SMS menjadi *query*.
- iv. Mengirimkan data SMS yang sesuai format ke aplikasi SMS-Banking di bank

Mengirimkan data SMS yang sesuai format dilakukan dengan menggunakan protokol TCP/IP (komunikasi melalui *socket*). Untuk itu, maka akan dilakukan komunikasi antar *socket* pada komputer aplikasi *SMS-Banking* dan *service provider*.
- v. Mengirimkan data SMS response transaksi dari bank ke nomor pelanggan

Hasil *request* dari pelanggan harus dapat dikirimkan kembali ke pelanggan dalam bentuk SMS. Untuk menunjang fungsi tersebut, maka perlu digunakan perangkat GSM *modem* yang dapat mengirimkan SMS ke nomor tertentu dengan menggunakan *AT Command*.

Spesifikasi kebutuhan perangkat lunak pada sis *server* untuk aplikasi *SMS-Baking* dan basis data bank secara umum terdiri dari :

- i. Menerima data SMS dari Bulk SMS Service Provider

Perangkat lunak *SMS-Banking* mampu menerima data dari *Bulk SMS Service Provider* dengan menggunakan komunikasi antar *socket*. Paket-paket data yang diterima harus dapat dibentuk kembali menjadi sebuah data SMS yang utuh beserta dengan tanda-tangan *digitalnya*.

ii. Membaca tanda-tangan digital dan melakukan otentikasi data SMS

Data SMS utuh yang diterima dapat dikenali bagian tanda-tangan *digitalnya* yang memiliki format khusus. Format tersebut secara umum adalah sebagai berikut :

```

<No-Seri><No-Rekening><Transaksi><Attribut
    Transaksi > ...
<s>letak tanda-tangan</s>

```

Contoh : a54e12cd12b 0028410018 CEK-SALDO

```

<s>ZXBS93ENWIL3292ANDJ2D</s>

```

Setiap data SMS akan terdapat tanda-tangan *digital* yang berada diantara tanda <s></s>. Hal ini digunakan untuk mempermudah proses pengidentifikasian tanda-tangan *digital* yang berasal dari komputer *server* di bank. Otentikasi dilakukan dengan kunci publik *server* yang tersimpan oleh pelanggan.

iii. Mendekripsi pesan transaksi yang penting (terenkripsi)

Untuk beberapa pesan yang mengandung data yang sangat penting seperti ubah PIN atau transaksi pendistribusian kunci publik dan kunci simetri ke bank, diperlukan kemampuan dari perangkat lunak *server* di bank yang dapat mendekripsikan pesan transaksi tersebut. Perangkat lunak akan mendekripsikan pesan dengan menggunakan kunci simetri yang telah dihasilkan oleh perangkat seluler pelanggan.

iv. Mengubah data SMS yang valid menjadi query ke basis data bank

Aplikasi mampu mengubah data SMS transaksi yang telah memenuhi keabsahan menjadi barisan *query* yang siap untuk *diinput* ke basis data bank. Dengan kata lain, aplikasi akan melakukan *update* basis data sesuai dengan *query* transaksi yang diproses.

v. Memberikan tanda-tangan digital untuk data SMS hasil request

Setiap hasil proses perbankan melalui SMS akan menghasilkan data hasil *request* yang berupa data SMS dan memiliki tanda-tangan *digital* di dalamnya.

Format yang digunakan untuk tanda-tangan *digital* kurang lebih sama dengan format dari data SMS yang diterima.

vi. Mengirimkan data SMS ke Bulk SMS Service Provider

Melalui komunikasi antar *socket*, maka aplikasi dapat mengirimkan hasil proses perbankan yang dilakukan ke *Bulk SMS Service Provider* berupa data SMS yang telah terdapat tanda-tangan *digitalnya*.

3.3.4 Batasan Perangkat Lunak

Adapun batasan perangkat lunak yang dibutuhkan untuk membangun sistem *SMS-Banking* diantaranya :

1. Perangkat lunak yang terdapat pada telepon seluler ini menyimpan 2 buah kunci, yaitu kunci-publik dan kunci privat yang tidak sepasang.
2. Jaringan GSM yang digunakan dianggap ideal dan handal sehingga SMS yang dikirimkan terjamin sampai pada *Bulk SMS Service Provider*.
3. Perangkat lunak *SMS-Banking* secara keseluruhan hanya dapat melakukan transaksi yang disebutkan sebelumnya. Mengenai transaksi lain seperti lima transaksi terakhir, pengisian pulsa, atau pembayaran tagihan telepon dan sejenisnya.
4. Basis data yang digunakan sebagai basis data bank merupakan basis data simulasi, bukan data bank yang riil. Nomor yang digunakan sebagai nomor untuk transaksi perbankan melalui SMS bukan merupakan nomor khusus seperti 9878, 9999, dan sejenisnya melainkan nomor GSM pada umumnya.

3.4 Analisis Keamanan dan Kelayakan Tanda-Tangan *Digital* dengan Fungsi *Hash* dan Algoritma RSA

Pada aplikasi *SMS-Banking*, terdapat penggunaan SMS yang merupakan representasi dari data transaksi yang digunakan oleh pelanggan dan bank. SMS ini memiliki

format tertentu yang telah dibahas pada subbab spesifikasi kebutuhan perangkat lunak sebelumnya. Data sms ini harus tetap terjaga kerahasiaannya (keasliannya) sampai pada saat pemrosesan dan peng-*update*-an basis data bank. Dengan kata lain, data SMS dari pelanggan maupun dari bank harus valid dan teruji keabsahannya.

Data SMS transaksi tersebut dianalogikan sebagai pesan rahasia dimana tidak boleh sembarang orang dapat mengetahuinya. Jaminan keamanan pesan ini tentunya ditangani oleh sistem kriptografi tertentu yang memiliki tingkat kesukaran tinggi. Saat ini sistem kriptografi yang memberikan jaminan keamanan pesan yang tinggi adalah sistem kriptografi kunci-publik dimana kunci rahasia yang digunakan pada sistem kriptografi ini sangat sukar untuk diturunkan dari kunci-publiknya. Sistem kriptografi inilah yang cocok digunakan untuk aplikasi *SMS-Banking*.

Salah satu sistem kriptografi kunci-publik adalah tanda-tangan *digital* dengan algoritma RSA. Tanda-tangan *digital* dengan algoritma RSA sangat tepat digunakan untuk otentikasi data *digital*, seperti pesan yang dikirimkan melalui saluran komunikasi dan dokumen elektronik. Tanda-tangan *digital* tersebut merupakan sistem kriptografi yang tergantung pada isi dokumen dan kunci. Tanda-tangan *digital* RSA direpresentasikan sebagai karakter-karakter heksadesimal dan ditaruh pada akhir SMS. Untuk membedakan tanda-tangan *digital* dengan isi SMS, maka tanda-tangan *digital* RSA diawali dan diakhiri dengan tag *<s>* dan *</s>*.

Kelayakan penggunaan algoritma RSA untuk tanda-tangan *digital SMS-Banking* dan keamanannya jika dibandingkan dengan DSA, ElGamal atau DES adalah sebagai berikut :

1. RSA sangat cocok digunakan untuk menangani pesan yang berukuran kecil seperti SMS. SMS tergolong sebagai pesan dengan ukuran kecil karena memiliki kapasitas maksimal hanya 160 karakter untuk satu SMS. Sedangkan DSA dan ElGamal lebih tepat untuk menangani pembentukan tanda-tangan *digital* dokumen yang berukuran lebih besar [LEO04].
2. Tingkat keamanan yang diberikan oleh algoritma ini cukup baik. Hal ini dapat dilihat dari tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $r = p \times q$. Selain itu, algoritma yang paling

mangkus untuk memfaktorkan bilangan yang besar belum ditemukan. Inilah yang membuat algoritma *RSA* tetap digunakan sampai dengan saat ini.

3. Dalam transaksi *SMS-Banking* lebih menekankan kepada otentikasi pesan SMS untuk transaksi selain kepada kerahasiaan pesan. Pihak bank cukup mengetahui bahwa data SMS yang diterimanya merupakan SMS dari pelanggan bank tersebut, begitu juga sebaliknya. Hal ini juga dikarenakan jaringan GSM sudah melakukan enkripsi pesan SMS selama pengiriman pesan dengan menggunakan algoritma kriptografi A5/1 atau A5/2. Dengan kata lain, penggunaan DES untuk menyimpan kerahasiaan pesan kurang signifikan penggunaannya.
4. Dengan menggunakan fungsi *hash*, tanda-tangan *digital* ini dapat menyelesaikan permasalahan *non-repudiation* (baik penerima dan pengirim pesan mempunyai pasangan kunci masing-masing). Penyelesaian tersebut merupakan solusi untuk permasalahan non teknis pada sistem *SMS-Banking* (permasalahan non teknis yaitu dimana operator bank bisa mengetahui kunci yang digunakan pelanggannya).

3.5 Analisis Protokol Komunikasi Kunci dalam Sistem *SMS-Banking*

Keamanan menjadi faktor yang sangat penting dalam proses transaksi *SMS-Banking*, termasuk pendistribusian kunci publik dan kunci simetri yang akan digunakan oleh pihak pelanggan dan pihak bank. Protokol yang digunakan harus jelas dan aman, sehingga pihak ketiga yang berusaha melakukan penyadapan transaksi tidak dapat melakukannya.

Pendistribusian kunci dalam pembahasan ini merupakan protokol kriptografi yang melibatkan dua belah pihak, yaitu pihak *client* (pelanggan) dan pihak *server* (bank), sedangkan untuk penyedia layanan nomor pendek (*service provider*) tidak termasuk dalam pihak yang terlibat karena fungsinya hanya sebagai perantara transaksi bukan perantara kunci. Pertukaran kunci awal dilakukan ketika pengguna mendaftarkan dirinya ke bank untuk layanan *SMS-Banking*. Untuk pertukaran selanjutnya diserahkan kepada pengguna.

Sebagai ilustrasi, maka pihak pelanggan akan dianggap sebagai *client* dan pihak bank akan dianggap sebagai *server*. Antara *client* dan *server* pada awal penggunaan aplikasi *SMS-Banking* akan saling bertukar kunci publik (pertukaran kunci ini dilakukan di saat pengguna melakukan registrasi layanan *SMS-Banking* ke bank). Kunci publik ini digunakan terutama dalam proses enkripsi kunci simetri yang dilakukan oleh *client* dan akan dikirimkan ke pihak bank. Transaksi *SMS-Banking* melibatkan kunci simetri untuk melakukan enkripsi terhadap pesan transaksi yang membutuhkan kerahasiaan isi pesannya (nomor seri pesan, ubah PIN, dan transfer uang). Secara lebih jelas, protokol komunikasi yang akan digunakan dalam pembahasan ini terdiri dari 3 bagian, diantaranya :

i. Protokol pertukaran kunci publik

- (1) Untuk menggunakan aplikasi *SMS-Banking* pada perangkat seluler, pihak *client* akan diberikan tampilan aplikasi untuk membangkitkan pasangan kunci privat dan kunci publik secara random.
- (2) Kunci privat yang dihasilkan akan disimpan dalam perangkat seluler *client*, sedangkan kunci publik akan dikirimkan ke pihak *server* melalui jaringan telepon seluler (GSM).
- (3) Ketika pihak *server* telah menerima kunci publik dari *client*, maka saat itu juga, *server* akan membangkitkan sepasang kunci privat dan publik *server*. Kunci privat *server* dan kunci publik *client* yang dihasilkan akan disimpan dalam tabel pemetaan kunci di komputer *server* (Tabel III-1). Selanjutnya, kunci publik *server* akan dikirimkan ke *client* melalui jaringan telepon seluler (GSM).

ii. Protokol pertukaran kunci simetri

- (1) Setelah menerima kunci public *client*, *server* akan membangkitkan kunci simetri untuk proses enkripsi pesan yang harus tersembunyi informasinya.
- (2) Kunci simetri yang dihasilkan akan disimpan dalam aplikasi *server* dan dikirimkan ke pihak *client* bersamaan dengan pengiriman kunci publik. Kunci

simetri yang dikirim akan dienkripsikan terlebih dahulu dengan menggunakan kunci publik *client* yang dimiliki oleh *server*.

- (3) Pihak *client* akan menerima kunci simetri yang terenkripsi tersebut dan mendekripsikannya dengan menggunakan kunci privat *client* yang dimilikinya. Pihak *server* akan menyimpan kunci simetri yang telah dibangkitkan tersebut dalam tabel pemetaan kunci simetri (Tabel III-2).

Tabel III-2 Pemetaan Kunci Simetri

No Telp	No Rekening	Kunci simetri
+6285220842578	112-121-2341	Abd23na1
+6285220075338	152-128-2643	7sad8s2sa
...

Berikut format SMS untuk pengiriman kunci :

<No-Rekening> <Nama-Transaksi> <Nilai –Kunci>

Contoh : 0028410018 KEY p:32178ab3a7c877d7a|n:76834aab7d7cba89a

Sedangkan format SMS hasil respon dari *SMS-Banking Server* adalah sebagai berikut :

<No-Rekening> <Nama-Transaksi> <Nilai –Kunci>

Contoh : 0028410018 KEY p:32178ab3a7c87d7a|n:76834ab7a8|s:36125acb8

iii. Protokol komunikasi transaksi melalui SMS

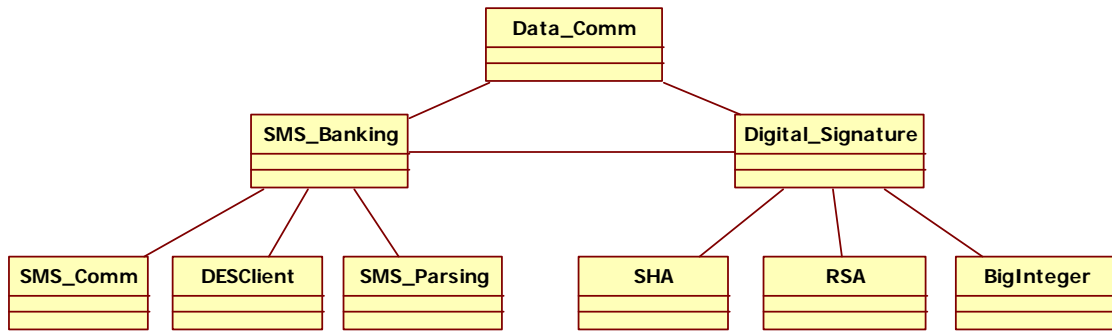
- (1) Untuk setiap pesan perbankan, *client* akan meringkas data SMS menjadi *message digest* dengan fungsi *hash* satu arah.
- (2) Pihak *client* mengenkripsi *message digest* dengan kunci privatnya. Hasil enkripsi tersebut akan disertakan sebagai tanda-tangan *digital* pada data transaksi SMS.
- (3) Untuk pesan yang mengandung informasi yang penting, maka pada bagian yang rahasia tersebut akan dienkripsi dengan kunci simetri terlebih dahulu lalu dienkripsikan dalam satu kesatuan data transaksi menjadi *message digest* seperti halnya butir diatas.

- (4) Pihak *client* mengirim data transaksi SMS yang sudah diberi tanda-tangan *digital* kepada pihak *server*.
- (5) Pihak *server* meringkas data transaksi SMS dari *client* menjadi *message digest* dengan fungsi *hash* yang sama. *Server* akan mendekripsikan tanda-tangan *digital* yang disertakan pada data transaksi SMS dengan menggunakan kunci publik *client*. Jika hasil dekripsinya sama dengan *message digest* yang dihasilkan, maka tanda-tangan *digital* tersebut sah.
- (6) Protokol ini juga berlaku sebaliknya, antara pihak *server* ke *client*.

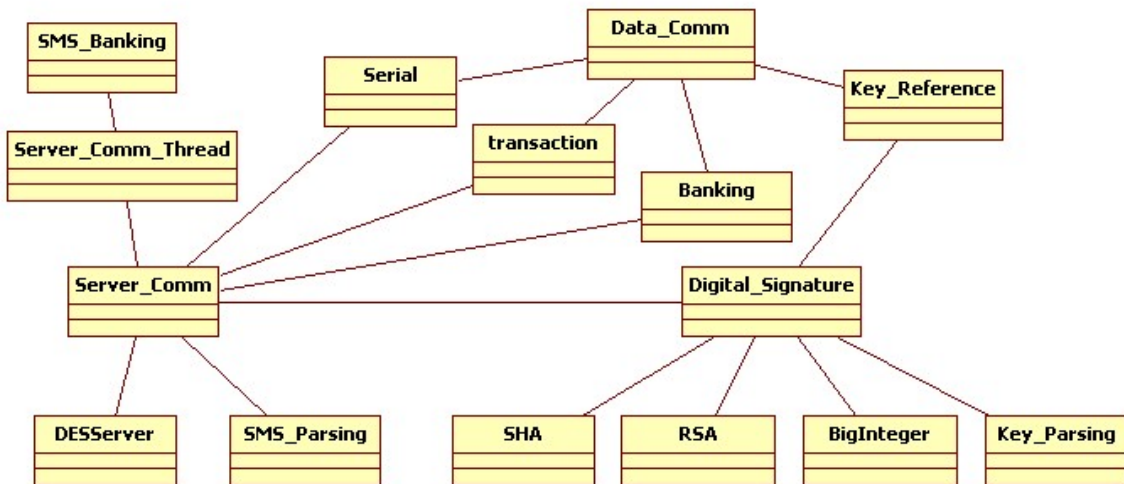
3.6 Diagram Kelas Analisis *Client-Server SMS-Banking*

Berdasarkan pembahasan sebelumnya dapat dihasilkan diagram kelas analisis untuk *client* pada Gambar III-5. Sedangkan untuk diagram kelas analisis *SMS-Banking Server* dan *Bulk SMS Service Provider* terdapat pada Gambar III-6 dan Gambar III-7. Setiap fungsi yang dibutuhkan oleh *Bulk SMS Service Provider* (verifikasi pesan SMS, pengecekan pelanggan terdaftar, dan sebagainya) harus dapat terimplementasikan dalam satu diagram kelas *Bulk SMS Service Provider*. Hal ini juga berlaku pada perancangan dan implementasi kelas yang lebih detail untuk diagram kelas *Bulk SMS Service Provider*.

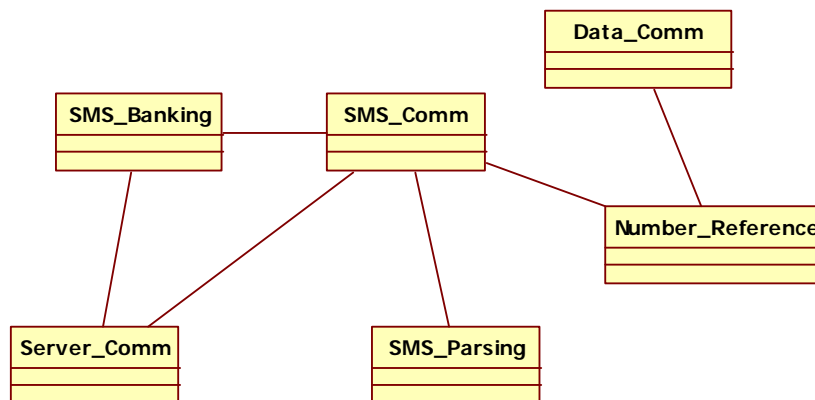
Diagram kelas *client* mencakup semua kelas yang merupakan komponen pembangun perangkat lunak *SMS-Banking* pada telepon seluler. Modul-modul yang terdapat di dalamnya akan dapat melakukan proses pembentukan tanda-tangan *digital* pada telepon seluler dengan keterbatasan yang ada. Komunikasi antara diagram kelas akan dianalisis berdasarkan bentuk data komunikasi yang dipertukarkan. Sebagai contohnya komunikasi antara *client* dengan *Bulk SMS Service Provider*. Komunikasi antara diagram kelas tersebut terjadi melalui data pesan SMS. Hal ini mengakibatkan kelas yang dibentuk harus dapat melakukan proses *transmitting* dan *receiving*.



Gambar III-5 Diagram Kelas Analisis Client



Gambar III-6 Diagram Kelas Analisis SMS-Banking Server



Gambar III-7 Diagram Kelas Analisis Bulk SMS Service Provider

Kelas **SMS_Banking** mengimplementasikan antarmuka perangkat lunak baik dari sisi *server* maupun *client*. Sedangkan untuk melakukan proses menerima dan mengirimkan SMS, akan diimplementasikan dengan menggunakan kelas **SMS_Comm**. Untuk melakukan proses pembentukan tanda-tangan *digital*, akan digunakan kelas **Digital_Signature** yang terhubung dengan kelas **RSA** (untuk implementasi algoritma RSA), kelas **SHA** (untuk implementasi fungsi *hash*), serta kelas **BigInteger**. Kelas **Key_Reference** akan melakukan operasi penyimpanan dan pengambilan informasi kunci publik *server* dan kunci privat *client*.