

Laporan Tugas Akhir Keamanan Sistem Informasi (EL-695)

**SMS SEBAGAI ALTERNATIF OTENTIKASI TRANSAKSI DI
INTERNET UNTUK MENCEGAH PENGGUNAAN CURIAN
NOMOR KARTU KREDIT**

Dosen: DR. Budi Rahardjo

Disusun Oleh:

**Nama : Firman Prima Djauhari
NIM : 23201067**

**Bidang Khusus Teknik Komputer
Program studi Magister Elektroteknik
Institut Teknologi Bandung
2003**

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT, yang telah memberikan rahmat dan karunia-NYA, sehingga penulis dapat menyelesaikan tugas akhir Keamanan Sistem Informasi berjudul “SMS Sebagai Alternatif Otentikasi Transaksi Di Internet Untuk Mencegah Penggunaan Curian Nomor Kartu Kredit ”.

Penulis mengucapkan terima kasih kepada Bapak Dr. Budi Rahardjo, selaku Dosen Mata kuliah Keamanan Sistem Informasi. Penulis berharap Tugas Akhir ini menjadi suatu informasi yang berguna bagi kita semua.

Penulis

DAFTAR ISI

Kata Pengantar	2
Daftar Isi	3
Abstrak	4
PENDAHULUAN	5
1.1 Latar Belakang	5
Tinjauan Pustaka	6
2.1 Teori	6
2.2 Teori Tambahan	8
Otentikasi melalui SMS	9
3.1 Otentikasi melalui SMS	9
Analisa	14
4.1 Analisis terhadap keamanan	14
4.2 Analisis Terhadap Privacy Pengguna	14
Kesimpulan	15
5.1 Kesimpulan	15

Daftar Pustaka

ABSTRAK

Carding merupakan salah kejahatan dalam dunia maya yang harus ditekan sekecil mungkin. Dampak yang ditimbulkan oleh Carding ini sangat besar terutama terhadap negara Indonesia antara lain: IP address Indonesia yang diblokir untuk transaksi atau untuk masuk ke situs tertentu, Kartu kredit dari Indonesia diblokir dan integritas pebisnis Indonesia turun. Dengan acuan ini maka salah satu untuk menangkal aksi para Carding ini adalah menggunakan SMS. SMS ini nantinya akan saling terkait antar pihak operator, penjual dan pelanggan.

Bab 1

PENDAHULUAN

1.1 Latar Belakang

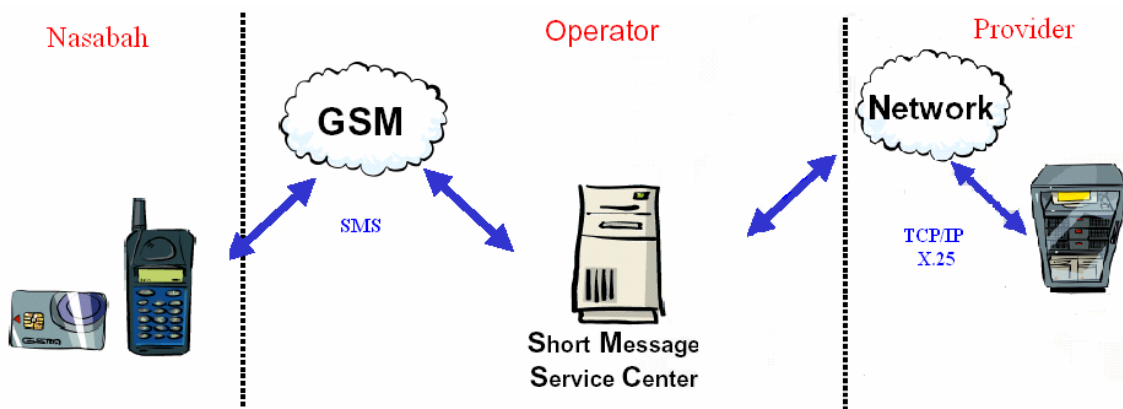
Kasus pencurian nomor kartu kredit merupakan suatu kejahatan intelektual yang tidak bisa dianggap remeh, hal ini terbukti Indonesia merupakan salah satu negara didunia yang dituduh melakukan transaksi secara illegal atau kita sebut istilah lain yaitu “CARDING”. Carding merupakan kejahatan yang tidak mengenal batas ruang dan waktu. Dengan carding ini banyak nasabah atau anggota kartu kredit sangat dirugikan dengan tindakan tersebut. Hukum yang adapun belum mampu mengatasi masalah carding ini.

Untuk mengatasi masalah tersebut adalah dengan melakukan antisipasi sebelum kerugian yang terjadi timbul. Short Messages Services(SMS) merupakan salah satu solusi dalam antisipasi kejahatan carding tersebut.

Bab 2 TEORI

2.1 Teori

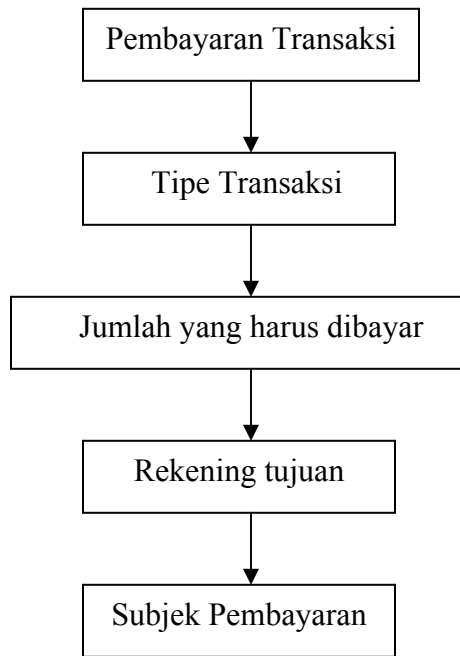
Pada dasarnya sms merupakan pesan tertulis yang dapat diterima dan dikirim ke pengguna handphone. Dengan adanya kerjasama antara bank dan operator seluler serta pengguna maka carding dapat diminimisasi sekecil mungkin. Bila seseorang menggunakan curian nomor kartu kredit dan melakukan transaksi diinternet maka bank akan membuat konfirmasi bahwa pada jam, hari, tanggal, tahun telah terjadi transaksi internet. Bila nasabah atau anggota kartu kredit tidak merasa melakukan transaksi internet maka berhak membatalkan transaksi tersebut. Untuk lebih jelasnya dapat dilihat pada gambar berikut:



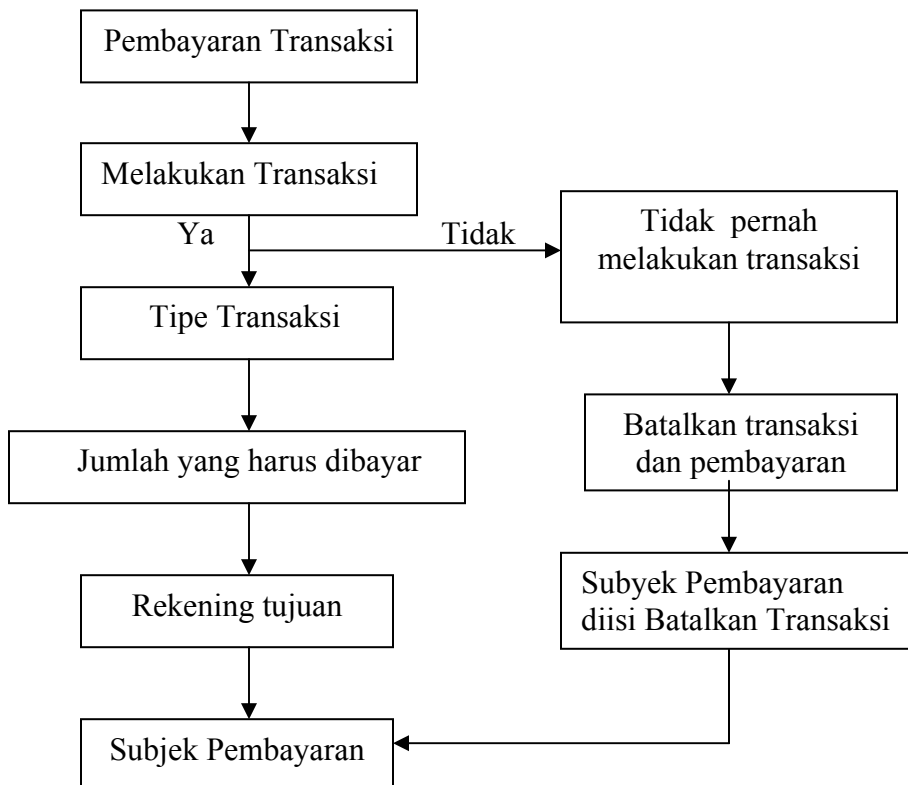
Dalam gambar tersebut bila seorang carding sedang melakukan carding maka provider dalam ini bank memberitahu ke nasabah menggunakan operator GSM melalui SMS. SMS tersebut dikirimkan ke nasabah untuk ditindaklanjuti. Untuk SMS sendiri harus mempunyai suatu menu yang interaktif bagi nasabah agar mudah dalam melakukan otentikasi.

Berikut ini Rancangan Menu SMS bagi nasabah:

- Pembayaran:
- Jumlah yang harus dibayar
- Tipe Transaksi
- Rekening tujuan
- Subjek Pembayaran



Bila nasabah tidak merasa melakukan transaksi maka dapat membatalkan transaksi tersebut sebagai berikut:



2.2 Teori Tambahan

SMS merupakan suatu pesan yang dikirim berdasarkan standar sinyal SS7 berisi teks singkat yang dikirim melalui SMS center.

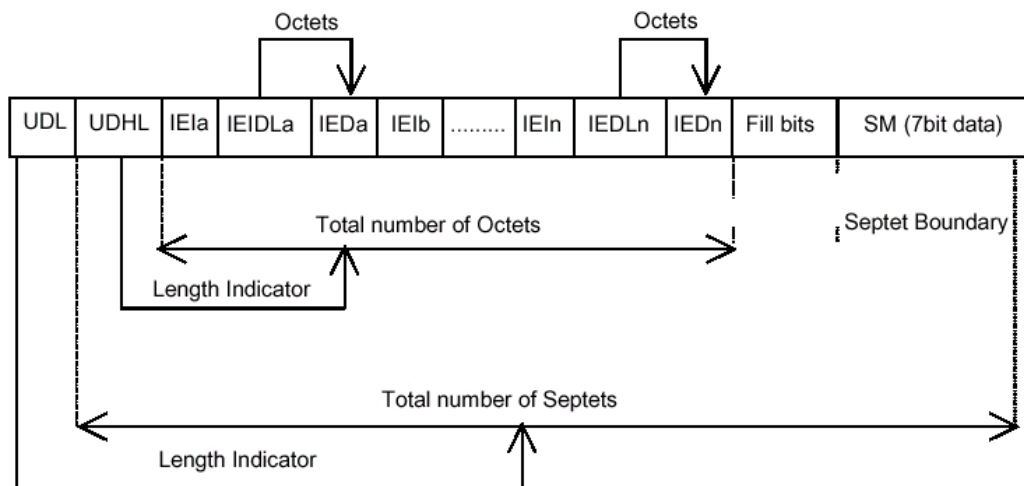
Adapun beberapa perintah yang dikenal dalam SMS yaitu:

- SMS-DELIVER (SC → MS)
- SMS-DELIVER-REPORT (SC ← MS)
- SMS-SUBMIT (MS → SC)
- SMS-SUBMIT-REPORT (MS ← SC)
- SMS-COMMAND (MS → SC)
- SMS-STATUS-REQUEST (MS → SC)

Arti singkatan:

- SC: Service Centre
- MS: Mobile Station

SMS terdiri dari Protocol Data Unit (PDU). Didalam PDU terdapat beberapa header yang sudah sesuai standar GSM 07.05.



SMS-Centre berfungsi sebagai routing dan mengirim SMS.

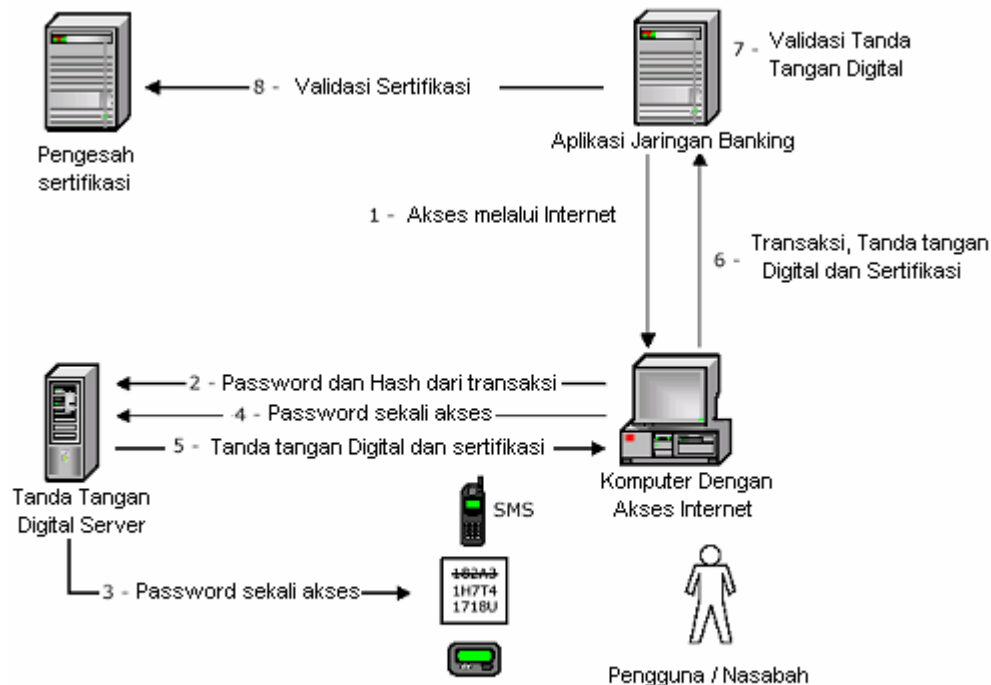
Bab 3

OTENTIKASI MELALUI SMS

3.1 Otentikasi melalui SMS

Dalam hal ini SMS bisa dijadikan sebagai otentikasi untuk mencegah para carding menggunakan kartu kredit ilegal. Untuk itu diperlukan suatu proses yang dapat memberikan pembuktian bahwa dengan cara otentikasi melalui SMS maka kejahatan carding dapat ditekan sekecil mungkin. Untuk itu diperlukan beberapa model yang dapat dijadikan acuan dalam implementasi otentikasi melalui sms tersebut.

Berikut ini otentikasi menggunakan validasi sertifikat dan tanda tangan digital:



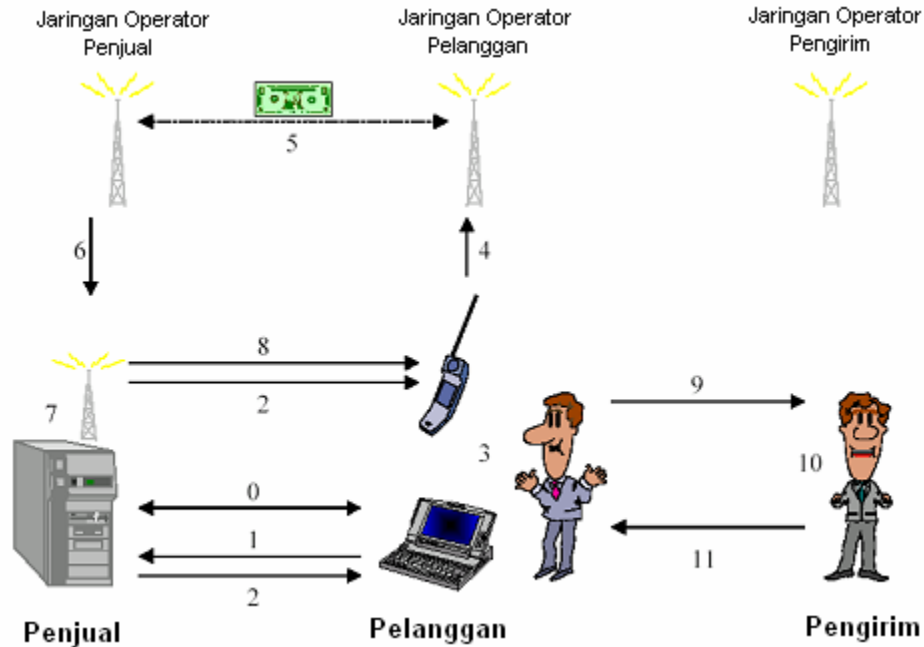
1. Untuk melakukan transaksi, pengguna mengakses terlebih dahulu bank tempat pengguna menyimpan rekening. Bank membutuhkan tanda tangan digital pengguna.
2. Password dibutuhkan untuk membentuk tanda tangan digital yang dikirim melalui saluran komunikasi yang aman.
3. Pengguna menerima password yang sudah berbentuk tanda tangan digital.
4. Pengguna mengirimkan password yang sudah berbentuk tanda tangan digital ke server menggunakan saluran komunikasi yang aman.

5. Server memberikan tanda tangan digital yang disertai sertifikat.
6. Semua transaksi, tanda tangan dan sertifikat sudah dikirimkan ke bank.
7. Bank kemudian memvalidasi tanda tangan digital dari pengguna.

Selain menggunakan tanda tangan digital dan sertifikat maka ada cara lain yang bisa dijadikan acuan dalam melakukan otentikasi melalui SMS yaitu proses-proses yang sifatnya membantu dalam validasi melalui SMS tersebut. Untuk lebih jelasnya maka dapat dilihat melalui Proses dalam melakukan transaksi melalui otentikasi SMS sebagai berikut:

- **Pelanggan** ingin membeli suatu barang melalui WWW dan membayar barang tersebut melalui GSM.
- **Penjual** menjual suatu barang melalui WWW dan menerima pembayaran melalui jaringan operator GSM.
- **Pengirim** akan melakukan pengiriman barang sesuai dengan permintaan pengiriman barang dari penjual.
- **Jaringan Operator** membantu Bank untuk melakukan pembayaran transaksi dari pelanggan ke penjual.

Dalam proses tersebut, setelah pelanggan melakukan pencarian terhadap suatu barang dan negosiasi harga maka pelanggan akan melakukan pembayaran. Penjual kemudian meminta pelanggan untuk pembayarannya melalui SMS. Pelanggan membayar sejumlah uang dan mengirimkannya ke operator jaringan, kemudian operator jaringan memberitahukan penjual bahwa transaksi sudah berhasil dibayar. Penjual mengirimkan tanda terima pembayaran ke pelanggan.



Proses (1)

0: Pencarian barang dan negosiasi

1: permintaan bertransaksi dengan world wide web (WWW)

- Format dan encoding dipilih oleh penjual
- Mengandung isi yang akan dibeli
- Deskripsi barang yang dibeli
- Jumlah uang yang harus dibayar
- Nomor GSM pelanggan
- Dikirim dengan format HTML
- Diproteksi dengan SSL/TLS

Proses (2)

2. Bertransaksi dengan konfirmasi SMS

Pesan Terdiri dari:

- Deskripsi barang
- Nomor Transaksi
- Nomor Transaksi penjual
- Jumlah uang yang harus dibayar
- Dan Dikirim juga dengan melalui WWW

Proses (3)

3. Verifikasi oleh pelanggan

- Hanya dengan SMS
- Membandingkan antara SMS dan WWW
- Verifikasi tanda tangan digital

4. Debit Rekening

- SIM aplikasi Toolkit

Pesan terdiri:

- Jumlah uang yang harus dibayar
- Nomor transaksi penjual

Proses (4)

5. Antara Jaringan Operator

- jaringan operator pelanggan Menentukan dan memastikan jumlah uang dari pelanggan
- Mengirimkan uang yang sudah di debit dari rekening pelanggan melalui jaringan operator pelanggan ke jaringan operator penjual
- Jaringan operator Penjual menambahkan jumlah uang ke rekening penjual

6. Pengiriman OK

Pesan terdiri dari

- jumlah uang yang harus dibayar

Proses (5)

7. Verifikasi oleh penjual

- verifikasi pengiriman Ok (6)
- Membandingkan konfirmasi penjualan (2)

8. Bukti pembayaran

- waktu dan tanggal bertransaksi
- Informasi untuk pengiriman
- Informasi untuk pelanggan

Proses (6)

9. Memperlihatkan bukti pembayaran

10. Verifikasi oleh pengiriman

11. mengirim barang

Bab 4 **ANALISA**

4.1 Analisis terhadap keamanan:

- penggunaan sistem keamanan antara web (www) dengan GSM sebaiknya Menggunakan keamanan SSL.
- walaupun masih terdapat masalah dengan keamanan ini, para carding tidak dapat melakukan pengecohkan terhadap dua sistem sekaligus dalam waktu yang bersamaan.
- Handphone dapat dikatakan merupakan keamanan yang privacy bagi penggunanya.

4.2 Analisis terhadap privacy pengguna:

- Nomor GSM tidak terlalu privacy dibandingkan dengan kartu kredit.
- Penjual mengetahui nomor GSM pelanggan (dengan asumsi nomor GSM tidak diberitahukan kepada pihak lain, jika dilakukan maka akan berlawanan dengan proses yang diatas)
- Operator jaringan mengetahui pelanggan yang melakukan transaksi suatu barang dari penjual

Bab 5

KESIMPULAN

5.1 Kesimpulan:

- Dalam menerima dan mengirim SMS konfirmasi sebaiknya disertai dengan tanda digital, hal ini untuk mengetahui dan menegaskan bahwa otentikasi berdasarkan teks dapat dipertanggungjawabkan.
- Dalam memberikan menu di SMS harus dilakukan hati-hati terutama harus ditekan sekecil mungkin terhadap software bug.
- Harus mudah diterapkan ke handphone atau ke SIM CARD lain (tidak tergantung oleh handphone atau SIM CARD tertentu).

DAFTAR PUSTAKA

- Giesecke & Devrient. *Secure Mobile Banking Applications*. STARTSIM Banking.
- Giesecke & Devrient. *Mobile Commerce*.
- Walter Carels. *Mobile Banking (SMS and WAP) via my KBC*. ICT Manager Electronic Banking. KBC.
- *Secure and Mobile Digital Signatures for Internet banking*. www.Cryptomathic.com.
- Oliver Zeller Secartis. *Mobile Security*. www.secartis.com.