

Pengantar Teknologi Mobile Banking

MOBILE BANKING

Adalah layanan perbankan yang dapat diakses langsung melalui telepon selular/*handphone* GSM (*Global for Mobile Communication*) dengan menggunakan SMS (*Short Message Service*).

Jenis Transaksi

- Transfer dana
- Informasi saldo, mutasi rekening, Informasi nilai tukar
- Pembayaran (kartu kredit, PLN, telepon, *handphone*, listrik, asuransi)
- Pembelian (pulsa isi ulang, saham)

Hal-hal yang perlu diperhatikan untuk keamanan transaksi *Mobile Banking*

- Wajib mengamankan PIN *Mobile Banking*
- Bebas membuat PIN sendiri. Jika merasa diketahui oleh orang lain, segera melakukan penggantian PIN.
- Bilamana *SIM Card* GSM Anda hilang/dicuri/ dipindahtangankan kepada pihak lain, segera beritahukan bank Anda terdekat atau segera telepon ke *Call Center* bank tersebut.

Mobile banking merupakan salah satu hasil pengembangan teknologi mobile yang digunakan dalam domain komersial. Mobil banking ini mengkombinasikan teknologi informasi dan aplikasi bisnis secara bersama. Berkat mobile banking, nasabah dapat menggunakannya untuk mendapatkan layanan perbankan 24 jam sehari tanpa harus mendatangi kantor cabang bank untuk transaksi personal. ***Mobile banking* merupakan layanan relative baru yang ditawarkan oleh perbankan terhadap pelanggannya dan karena kenyamanan dan fitur yang menghemat waktu, pelanggan menghargai layanan tersebut (Suoranta, 2003).**

Mobile banking merupakan salah satu layanan perbankan yang menerapkan teknologi informasi. Layanan ini menjadi peluang bagi bank untuk menawarkan nilai tambah sebagai insentif kepada pelanggan. Promosi *mobile banking* akan memberikan implikasi secara langsung pada adopsi yang dilakukan konsumen terhadap teknologi. *Mobile banking* atau biasa disebut *M-Banking* merupakan suatu layanan perbankan yang diberikan pihak bank untuk mendukung kelancaran dan kemudahan kegiatan perbankan. Serta keefektifan dan keefisienan nasabah untuk melakukan berbagai transaksi. *M-banking* tidak akan berjalan jika tidak didukung oleh suatu alat sebagai media untuk melakukan *mobile banking*. Media komunikasi yang dapat dipergunakan adalah telepon seluler atau ponsel. Dengan fasilitas ini, setiap orang yang memiliki ponsel dapat dengan mudah bertransaksi dimana saja dan kapan saja.

Dibandingkan layanan e-banking lainnya, perkembangan mobile banking (m-banking) terbilang paling cepat. Perkembangan ini lantaran kehadiran layanan m-banking mampu menjawab kebutuhan masyarakat modern yang sangat mengedepankan mobilitas. Dengan satu sentuhan, m-banking menciptakan kemudahan layanan perbankan dalam satu genggam. Kebermanfaatan dari layanan mobil banking akan meningkatkan kepuasan nasabah. Lebih jauh, mobile banking menciptakan “nilai” bagi transaksi nasabah bank sebagai channel penyampaian jasa nirkabel (*wireless*).

Tidak dapat dipungkiri bahwa perkembangan teknologi khususnya teknologi perbankan memaksa industri perbankan untuk memformulasi ulang strategi Teknologi Informasi yang mereka terapkan untuk tetap bisa bersaing. Nasabah sekarang menginginkan sesuatu yang lebih dari sekedar layanan perbankan. **Nasabah menginginkan kenyamanan dan fleksibilitas (Birch and Young, 1997; Lagoutte, 1996)** pada produk dan jasa yang sesuai kebutuhan mereka serta mudah digunakan yang tidak bisa ditawarkan oleh perbankan tradisional. Di masa depan e-banking akan menjadi aplikasi strategis yang penting untuk bersaing yang harus ditawarkan oleh seluruh bank dan institusi keuangan.



Gambar : Contoh Aplikasi Mobile Banking

PHONE BANKING

Adalah layanan yang diberikan untuk kemudahan dalam mendapatkan informasi perbankan dan untuk melakukan transaksi finansial *non-cash* melalui telepon.

Jenis Transaksi

- Transfer dana
- Informasi saldo, mutasi rekening
- Pembayaran (kartu kredit, PLN, telepon, *handphone*, listrik, asuransi)
- Pembelian (pulsa isi ulang)

Hal-hal yang perlu diperhatikan untuk keamanan transaksi *Phone Banking*

- Wajib mengamankan PIN *Phone Banking*
- Bebas untuk membuat PIN sendiri. Jika merasa diketahui oleh orang lain, segera lakukan penggantian PIN.

SMS BANKING

Adalah layanan informasi perbankan yang dapat diakses langsung melalui telepon selular/*handphone* dengan menggunakan media SMS (*short message service*)

Jenis Transaksi :

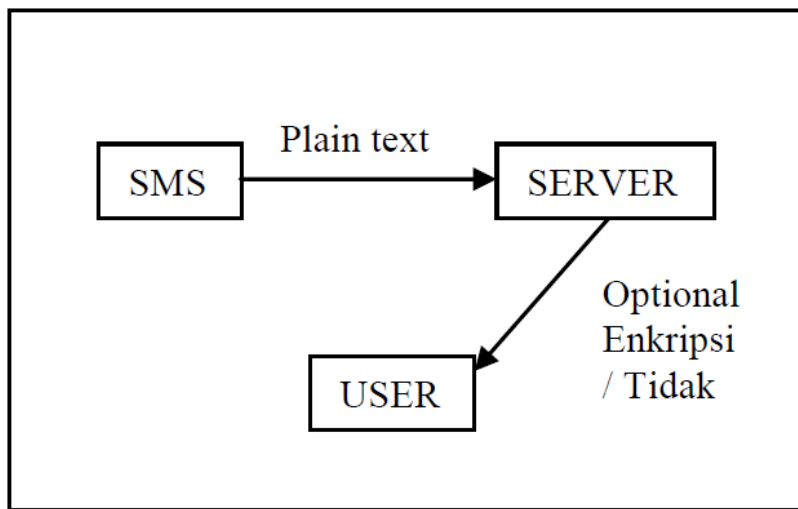
- Transfer dana
- Informasi saldo, mutasi rekening
- Pembayaran (kartu kredit)
- Pembelian (pulsa isi ulang)

Hal-hal yang perlu diperhatikan untuk keamanan transaksi *SMS Banking*

- Jangan memberitahukan kode akses/nomor pribadi *SMS Banking* kepada orang lain
- Jangan mencatat dan menyimpan kode akses/nomor pribadi *SMS Banking* di tempat yang mudah diketahui oleh orang lain.
- Setiap kali melakukan transaksi melalui *SMS Banking*, tungguilah beberapa saat hingga menerima response balik atas transaksi tersebut.
- Untuk setiap transaksi, akan menerima pesan notifikasi atas transaksi berupa SMS yang akan tersimpan di dalam inbox.

Beberapa bank sudah menerapkan SMS Banking menjadi salah satu fiturnya. Pengguna cukup mengetikkan kode tertentu untuk melakukan transaksi dan dikirimkan melalui SMS. Saat SMS dikirimkan, pesan tidaklah dienkripsi. Lalu SMS tersebut diterima oleh server, seperti SMS Gateway, kemudian oleh server diambil data yang dimaksudkan. Saat mencari dan mengambil data yang dibutuhkan data dienkripsi. Saat pengiriman data yang dimintai oleh pengguna dapat dienkripsi terlebih dahulu atau tidak saat dikirimkan kembali, hal ini bergantung dengan kesepakatan antara developer dan provider.

Untuk metode enkripsi yang digunakan juga bisa apa saja tergantung kebutuhan dan permintaan user (client). Jika melakukan enkripsi saat pengiriman data ke pengguna maka akan membutuhkan biaya yang lebih.



Gambar : Skema sederhana SMS Banking

Analisis keamanan pada SMS Banking,

1. Plainteks (berkas ASCII atau teks biasa (bahasa Inggris: '*plain text*')) SMS dikirimkan melalui protokol GSM yang hanya dienkripsi menggunakan algoritma A5 (*Algoritma A5* merupakan algoritma yang digunakan untuk melakukan enkripsi pada pensinyalan data dan suara dari mobile station/ponsel ke BTS), akan tetapi ada juga protokol GSM yang tidak melalui proses enkripsi terlebih dulu, sehingga semakin rawan saat pertukaran data terjadi. Algoritma A5 bukan merupakan enkripsi yang aman, karena peneliti telah membuktikan bahwa algoritma tersebut dapat ditembus dan tidak tahan terhadap serangan.
2. SMS yang menunggu untuk dikirim disimpan di store di dalam penyedia layanan yang berupa plaintexts. Meskipun setelah pesan terkirim, penyedia layanan menyimpan semua pesan. Jika isi pesan tidak dienkripsi maka orang lain yang mendapatkan akses ke provider bisa melihat data yang bersifat privasi milik pengguna.
3. USSD banking (*USSD* or *Unstructured Supplementary Service Data*). Verifikasi tergantung hanya pada nomor pengirim, jika SIM card hilang atau diduplikasi, maka penyerang dapat menggunakan akun korban yang melakukan transaksi. Pesan USSD yang dikirimkan ke server bank hanya dienkripsi antara mobile station dan base receiver station. Pesan adalah plaintexts yang ada di dalam jaringan operator telepon.
4. Pin autentifikasi. Bank menggunakan USSD untuk memperbolehkan konsumen mereka mengirimkan autentifikasi pin. Penyedia layanan dapat membaca Pin karena dikirimkan berupa plaintexts.
5. Beberapa SMS Banking menggunakan WIG (*wireless internet gateway-STK applications*) dengan SIM menu sebagai aplikasi. Jika aplikasi ini dimuat ke dalam SIM card maka membuat aplikasi mobile banking SIM card dependent. Jika SIM card hilang, maka keamanannya terancam.

Referensi:

1. <http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Makalah1/Makalah1-IF3058-Sem1-2010-2011-007.pdf>
2. <http://repository.unhas.ac.id/bitstream/handle/123456789/600/Proposal.pdf?sequence=2>
3. <http://www.gadgetflazz.com/bca-mobile-untuk-blackberry/>