

PROPOSAL TUGAS AKHIR
MATA KULIAH KEAMANAN SISTEM LANJUT (7010)
Dosen : Dr. Budi Rahardjo

**DIGITAL SIGNATURE DENGAN SUBSCRIBER WAP IDENTIFY MODULE
UNTUK PENGAMANAN M-BANKING**

Nama Mahasiswa : I Gusti Made Ardana

NIM : 23202129

Abstraksi

Peningkatan penggunaan Handphone di Indonesia yang mencapai angka 2 juta pada tahun 2002 dan dipredikasi naik sekitar 30% pada tahun 2003 merupakan sebuah kemajuan yang sangat pesat di dibandingkan dengan penggunaan alat komunikasi yang lain dalam kurun waktu yang sama. Peningkatan ini di antisiapasi oleh perbankan di Indonesia dengan menggandeng operator seluler untuk mengadakan fasilitas *m-banking*

Fasilitas *m-banking* mampu meningkatkan transaksi yang terjadi pada bank tersebut. Salah satu contohnya adalah fasilitas *m-banking* BCA yang mencatat volume bisnis Rp 151 miliar per September 2001, pada akhir 2002 sudah mencapai angka Rp 2,13 triliun. BCA merupakan salah satu contoh sukses dunia perbankan dalam mengimplementasikan teknologi informasi.

Salah satu isu utama yang sering menjadi bahan diskusi adalah sisi keamanan dalam transaksi yang menggunakan teknologi informasi. Hal ini memang cukup beralasan sebab transaksi dengan model ini sangat rentan terhadap kesalahan apabila sistem yang diterapkan tidak tepat. Model pengamanan pada Internet Banking dengan Jaminan SSL 128 bit inilah yang sering digunakan dalam iklan dan dalam meyakinkan kustomer. Kata-kata lainnya yang sering digunakan dalam menjamin keamanan para pengguna adalah penggunaan firewall, *Public Key Infrastructure* dan *Encryption Accelerator Card*.

Paper ini akan mencoba membahas salah satu teknik pengamanan *m-banking* yang diperkenalkan oleh perusahaan Schlumberger adalah teknik pengamanan menggunakan *Digital Signature* dengan *Subscriber WAP Identify Module*.

Daftar Rujukan :

- [1] L.M.S.C. of the UEEE Computer Society. Wireless LAN medium accses control (MAC) and physical layer (PHY) spesification IEEE Stabdard 892.11, 1999 edition,1999
- [2] GOST 34.10 - 94, "Information Technology Cryptographic Data Security Produce and Check procedures of ElectronicDigital Signature based on Asymmetric Cryptographic Algorithm", (1994).
- [3] <http://www.mysecuresign.com/archives/01-31-2003.htm>
- [4] <http://www.smarttrust.com/banking/default.asp>
- [5] <http://www.slb.com/press/company/whitepapers/#it>

Bandung, 9 Oktober 2003
Menyetujui,

Dr. Budi Rahardjo