KEAMANAN DAN PERLINDUNGAN NASABAH *ELECTRONIC BANKING*

Oleh:
RATNA NURHAYATI, SH, M.Hum
NIP. 132205566

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS TERBUKA
2004

LEMBAR PERSETUJUAN

Makalah dengan

Judul : KEAMANAN DAN PERLINDUNGAN NASABAH *ELECTRINIC BANKING*

Oleh : Ratna Nurhayati, S.H.,M.Hum

NIP : 132 205 566

Ini telah ditelaah dan disetujui secara materi oleh Ahli Materi

Mengetahui

Kajur Ilmu Administrasi,

Drs. Darmanto, M.Ed

NIP. 131 602 651

Ahli Materi,

Drs. Mirza Pahlevi, MM

NIP. 132 044 756

BAB I. LATAR BELAKANG PERMASALAHAN

Institusi perbankan dewasa ini telah banyak dipengaruhi oleh pengembangan produk teknologi informasi. Inovasi-inovasi teknologi informasi seperti *e-commerce, e-banking, e-money*, dan lain sebagainya telah mengubah pola dan cara perbankan maupun masyarakat dalam berinteraksi dan bertransaksi.

Hasil riset majalah info bank menunjukkan bahwa 58,41 persen bank sudah on line, dan dari 150 bank di Indonesia, terdapat 49 bank atau 43,6 persen yang benar-benar telah memiliki jaringan ATM. (Kusumaningtuti S.S., 2001)

Penyelenggaraan jasa perbankan melalui internet di Indonesia sejak 1999. Pada tahun 2001 sudah terdapat 6 bank penyelenggara internet banking : Bank Lippo, BCA, Bank Bali, BII, Bank Universal, dan Bank Niaga sedangkan bank lain yang akan menyelenggarakan internet banking diantaranya Bank Mega, Standard Chartered Bank.

No.	Nama Bank	Jumlah Nasabah Per April 2001
1	BII	40,838
2	BCA	99,504
3	Bank Bali	4,188
4	Bank Lippo	9,845
	TOTAL	154,375

(Sumber : Maman H. Soemantri, 2001)

Electronic Banking (e-banking) ini timbul sebagai akibat dari tuntutan nasabah akan layanan yang cepat, selalu "on" dan tersedia 24 jam/hari dan adanya peluang bisnis. Dari

sisi nasabah *e-banking* secara nyata telah mempermudah penggunaan jasa perbankan, memberikan keleluasaan waktu pelayanan, menyediakan kecepatan dan ketepatan pelayanan, dan menyediakan keanekaragaman jenis pelayanan. Dan dari sisi perbankan, e-banking diyakini mampu membuka peluang munculnya produk baru dan sekaligus mendorong nasabah agar lebih aktif menggunakan jasa bank. (Kusumaningtuti S.S., 2001)

Selain kemudahan di atas, ternyata *e-banking* juga mengandung resiko. Bambang Suherman, salah satu nasabah bank Lippo cabang Ungaran-Semarang, menceritakan pengalaman tentang 'nasib' tabungannya di bank tersebut pada Surat Pembaca di harian Suara Merdeka..

Pada tahun 1996 Bambang sudah menjadi nasabah di bank Lippo cabang Ungaran-Semarang, tetapi sejak Mei sampai 21 Oktober 2002 dia tidak pernah menabung atau mengambil uang lewat ATM (Anjungan Tunai Mandiri) sehingga cara menggunakan dan nomor PIN-nya pun lupa.

Anehnya, pada tanggal 22 Oktober 2002 saat dia menabung dan memeriksa buku tabungannya, tertera pengambilan lewat ATM pada awal Juli 2002 sebesar Rp. 5 juta, 29 Juli sebesar Rp. 2.750.000, tanggal 31 Juli sebesar Rp. 1 juta, tanggal 1 Agustus sebesar Rp. 1juta, dan terakhir tanggal 2 Agustus sebesar Rp. 1 juta, sehingga Bambang kehilangan uangnya total sebesar Rp. 11.750.000,- Padahal pada tanggal-tanggal tersebut Bambang sedang berada di Jakarta sedangkan data komputer bank menyebutkan uang diambil di Yogyakarta dan Semarang.

Bambang juga mempunyai pengalaman lain yaitu ada orang lain berbelanja di salah satu Mall di Semarang menggunakan kartu ATM dengan kode PIN milik Bambang. Namun,

karena tanda tangan orang tersebut tidak sama dengan tanda tangan Bambang, sehingga transaksi tersebut ditolak. Pengalaman-pengalaman pahit tersebut membuat Bambang hilang kepercayaan pada Bank Lippo. *(Suara Merdeka, 16 Nopember 2002)*

Kasus lain menimpa Christiana Kuki Palupi, salah seorang nasabah Bank Mandiri Cabang Pondok Bambu II Jakarta Timur, yang melakukan tiga kali transaksi tetapi saat transaksi yang ketiga ATM mati karena saat itu wilayah Pondok Bambu listrik padam. Sekitar 15 menit kemudian, ATM Mandiri kembali berfungsi tetapi kartunya tertelan dan transaksi yang terekam sebanyak empat kali sedangkan dia hanya berhasil melakukan transaksi dua kali dengan uang sebesar Rp. 1.000.000,-. *(Kompas Cyber, 26 April 2002)*

Selain kasus Bambang dan Christiana di atas, dunia perbankan melalui Internet (*internet banking*) di Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan *internet banking* Bank Central Asia (BCA).

Steven membeli domain-domain mirip www.klikbca.com (situs asli *internet banking* BCA), yaitu domain wwwklikbca.com, kilkbca.com, clikbca. com. klickbca.com dan klikbac. com. Isi situs-situs "plesetan" ini pun nyaris sama, kecuali tidak adanya *security* untuk bertransaksi dan adanya formulir akses (*login form*) palsu. Jika nasabah BCA salah mengetik situs BCA asli dan masuk 'perangkap' situs plesetan Steven, identitas pengguna (*user id*) dan nomor identifikasi personal (PIN) dapat ditangkap Steven. (Heru Sutadi, 2001)

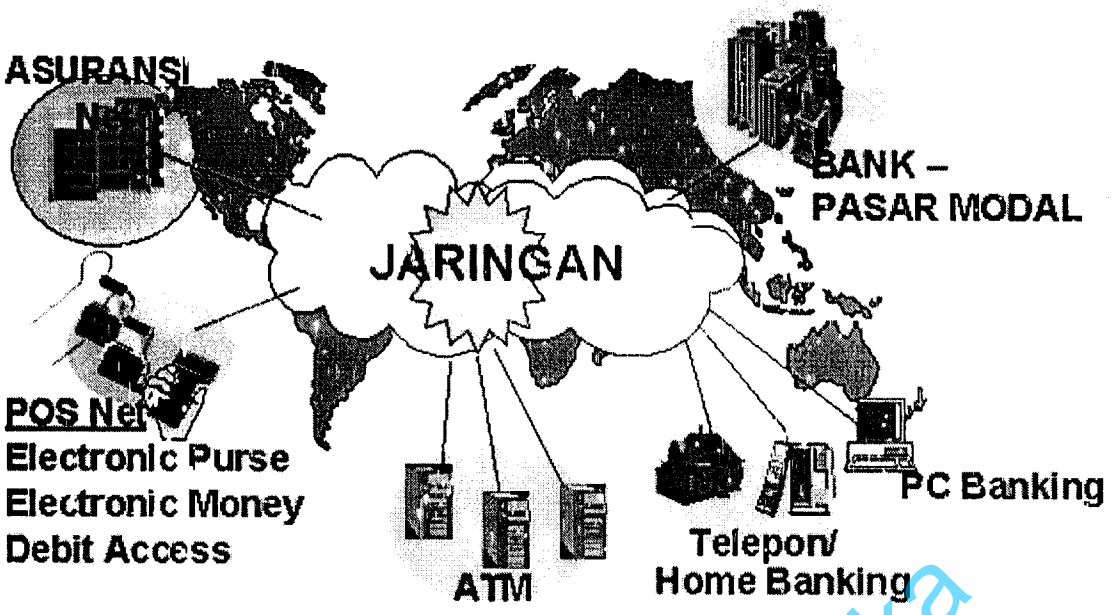
BAB II. PERMASALAHAN

Berdasarkan latar belakang permasalahan tersebut di atas, yang menjadi permasalahan dalam makalah ini adalah : apakah aman transaksi perbankan yang dilakukan melalui *e-banking* itu ? bagaimana perlindungan nasabah yang menderita kerugian akibat transaksi *e-banking* ?

BAB III. PEMBAHASAN

Dalam pandangan umum, *e-banking* adalah sebuah bentuk aplikasi teknologi informasi (TI) di sebuah bank, diselenggarakan untuk mempermudah layanan perbankan. Dalam pengoperasiannya, e-banking akan mempergunakan internet, yang apabila kita kaji lebih mendalam terdapat 2 makna atau arti dari 'Internet', yaitu ditinjau dari sisi teknologi dan jaringan (Budi Rahardjo, 2001). Teknologi Internet adalah teknologi komunikasi yang berbasis kepada protokol TCP/IP, dan juga penggunaan web browser sebagai user interface. Sementara itu pengertian Internet sebagai jaringan adalah jaringan komputer yang terbesar di dunia. Ada jaringan komputer lain yang bukan Internet, seperti misalnya jaringan privat dari beberapa perusahaan yang besar.

Secara umum interaksi sektor perbankan dan keuangan melalui internet dapat digambarkan sebagai berikut :



Gambar: Interaksi Sektor Perbankan dan Keuangan Melalui Internet
(Sumber : Taufik Akbar dkk-editor, 1998)

A. INTERNET BANKING

Pelayanan jasa keuangan berbasis internet merupakan jalur distribusi baru yang digunakan oleh kalangan perbankan di Indonesia dalam memenuhi tuntutan persaingan global perbankan di masa kini dan di masa depan. (Syahril Sabirin, 2001)

Menurut Maman H. Soemantri, ada 5 (lima) aspek dalam internet banking, yaitu:

a. perijinan
b. prudential management
c. risk management
d. consumer protection
e. aspek hukum

Aspek hukum terkait pengaturan Internet Banking, yaitu :

a. Keabsahan transaksi dan kekuatan pembuktian

b. Sanksi pelanggaran

c. *Security/ privacy breaches*

d. *Cross border issues*

Lebih lanjut Maman H. Soemantri menjelaskan bahwa internet banking memberikan keuntungan baik kepada nasabah maupun institusi perbankan itu sendiri, yaitu:

- Dari Sisi Bank :

a. Menekan *overhead cost*

b. Meningkatkan kualitas pelayanan bank lebih baik dan efisien

c. Meningkatkan competitiveness bank

- Dari Sisi Nasabah : Meningkatkan kenyamanan dan kecepatan transaksi tanpa batasan ruang dan waktu, bersifat global lintas negara.

Dalam praktek terdapat beberapa macam fungsi e-banking (bentuk layanan *internet banking*), yaitu : (Kusumaningtuti S.S dan Maman H. Soemantri, 2001)

- Fungsi Informasi *(Informational Website)*

Ini merupakan tingkatan dasar terhadap penggunaan teknologi internet banking. Bank mempergunakan e-banking hanya untuk memasarkan produk dan jasanya melalui website dengan mempergunakan server yang biasanya dikelola sendiri oleh Bank. Risiko dalam tingkatan ini sangat rendah, mengingat tidak terdapat hubungan langsung antara layanan informasi yang diberikan bank tersebut dengan jaringan operasional intern bank dalam memberikan layanan kepada nasabah.

- Fungsi Komunikasi *(Communicative Website)*

Penggunaan internet banking disamping untuk informasi juga memungkinkan adanya komunikasi dengan konsumen melalui sistem yang dipergunakan. Fasilitas yang disediakan bagi konsumen biasanya berupa e-mail, layanan keterangan rekening nasabah, formulir-formulir pembukaan tabungan/pinjaman dll. Dalam tingkatan ini terdapat risiko yang lebih besar karena telah terdapat hubungan (koneksi) dengan jaringan operasional intern bank dalam layanan kepada nasabah.

- Fungsi Transaksional *(Transactional Website)*

Dalam tingkatan ini, konsumen diberi keleluasaan untuk melakukan transaksi, seperti membayar tagihan, transfer, penarikan dan lain-lain. Sehubungan dengan hal tersebut dalam tingkatan ini sangat dibutuhkan kontrol yang sangat kuat dan keamanan terhadap penggunaan teknologi ini. Oleh karena itu bank yang akan menyelenggarakan internet banking pada tingkatan ini perlu mengajukan ijin kepada Bank Indonesia.

Apabila masalah keamanan ini tidak dikontrol dengan sangat ketat, celah *security* ini dapat diterobos oleh pihak yang tidak bertanggung jawab dengan bermacam-macam teknik, yaitu (I Made Wiryana dan Tedi Heriyanto, ...) :

- **Ticker symbol smashing**. Biasanya digunakan pada pengumuman *press release*, dengan memanfaatkan simbol dari perusahaan besar lainnya. Sehingga secara tersamar pengguna akan belok ke situs ini. Misal Perusahaan KUMBAYO baru saja meluncurkan produknya. Perusahaan ini tak ada hubungan dengan ***Bank Ha Ha***. Misal Bank Ha-Ha adalah suatu bank besar. Dengan cara ini orang akan terdorong ke situs perusahaan KUMBAYO, yang semula akan ke Bank Ha-Ha.

- **Web Spoofing** (Felten et al, 1997). Memanipulasi alamat URL pada sisi client, sehingga akan memaksa si korban melakukan browsing dengan melalui situs tertentu terlebih dahulu. Dengan cara ini dapat menyadap segala tindakan si korban, ketika melakukan akses ke situs-situs. Sehingga si penyerang dapat memperoleh PIN ataupun password. Cara ini biasanya memanfaatkan trick **URL Rewrite**. Umumnya pengguna awam tak memperhatikan apakah akses dia ke suatu situs melalui `http://www.yahoo.com` ataukah melalui `http://www.perusak.org/http://www.yahoo.com`. Karena yang tampil di browsernya adalah tetap halaman dari www.yahoo.com

- **DNS Spoofing** (Bellovin, 1995). Teknik ini digunakan untuk memanfaatkan DNS server untuk membangkitkan celah sekuriti. Dengan cara ini penyerang mampu membelokkan seorang pengguna ke server DNS lain yang bukan server semestinya, ketika ia memasukkan nama situs. Dengan cara ini maka penipuan dapat dilanjutkan misalnya dengan mengumpulkan PIN atau password.

- **typo pirates**. Dengan cara mendaftar nama domain yang hampir mirip, dan membuat situs yang mirip. Pengguna yang tak waspada akan masuk ke situs ini dan memberikan PIN dan password. Cara inilah yang terjadi pada kasus KlikBCA palsu. Hal ini disebabkan sebagian besar pengguna tak waspada, apakah alamat URL (*Universal Resource Locator*) yang dimasukkannya benar pada saat ia mengakses suatu situs web, dan apakah sertifikat yang diterima sama dengan sertifikat seharusnya pada saat ia mengakses situs web yang mendukung SSL.

- **cybersquating**. Membeli nama *domain* yang mungkin akan digunakan orang. Tujuan penggunaan cara ini adalah lebih kepada mengambil keuntungan keuangan dengan menjual kembali domain tersebut pada harga yang jauh lebih tinggi daripada harga sebenarnya.

- **Man-in-the-middle-attack**. Cara ini dilakukan dengan memaksa orang percaya bahwa situs yang dituju sama halnya dengan situs asli. Hal itu dilakukan dengan mencegat akses pengguna ketika hendak melakukan koneksi ke situs asli, teknik seperti **TCP Hijack** sering digunakan, lalu meneruskan akses pengguna ke web situs sebenarnya. Sepintas lalu hal ini tidak terlihat oleh pengguna. Serangan ini lebih berbahaya daripada sekedar *typo pirates*. Resiko ini bisa timbul ketika jalur penyerang berada di antara pengguna dan situs penyedia layanan.

B. KEAMANAN *(SECURITY) ELECTRONIC BANKING*

Keamanan adalah salah satu kunci utama keberhasilan operasional sektor perbankan. Tidak ada satupun bank yang merelakan informasi yang dimiliki oleh perusahaannya diketahui dan diambil oleh pihak lain. Seiring dengan berpindahnya metode informasi perbankan dari bentuk kertas ke bentuk elektronis yang memberikan tingkat effisiensi penggunaan yang jauh lebih baik dari bentuk kertas, maka untuk selanjutnya pengontrolan keamanan lembaga perbankan harus dititikberatkan pada pengamanan informasi elektronis tersebut. Dalam hal keamanan, tidak seperti informasi dalam bentuk kertas, maka informasi elektronis dapat dicuri atau dibaca dari tempat yang jauh dari tempat informasi itu berada.

Keamanan informasi menggambarkan seluruh aturan yang dilakukan untuk mencegah penggunaan yang tidak bertanggung jawab seperti pengeksposan, pengubahan, penggantian atau perusakan dari data yang disimpan secara elektronis. Saat ini kebutuhan yang diperlukan untuk melakukan pengamanan elektronis tersebut telah sepenuhnya dipahami. Pengamanan informasi elektronis diklasifikasikan sebagai penyediaan tiga jasa, yaitu :

1. Kerahasiaan dan Privasi

   Penyembunyian data dari pihak yang tidak berhak, sehingga memberikan privasi kepada pemilik data tersebut.

2. Keaslian

   Jaminan bahwa data yang diberikan adalah data yang asli

3. Ketersediaan

   Jaminan bahwa walaupun telah diberikan pengamanan tambahan data asli tetap dapat diakses oleh pihak yang berwenang

Untuk pelaksanaan pengamanan elektronis ini, dapat dilakukan pada 3 tingkatan yang berbeda :

1. Pengamanan Sendiri

   Dengan sistem pengamanan seperti ini, seluruh transaksi dan informasi yang disediakan tanggung jawab pengamanannya dilakukan sendiri oleh bank atau institusi keuangan lainnya. Dengan metode seperti ini suatu institusi dapat menentukan sendiri aturan yang akan diterapkan sepanjang tidak melanggar apa yang telah ditentukan regulator sebagai pengatur seluruh aktivitas.

2. Pengamanan Bersama

Sistem ini biasanya dilakukan oleh beberapa bank atau institusi yang mempunyai aturan yang ditetapkan bersama dalam pengoperasian suatu sistem tertentu. Tanggung jawab pengamanan informasi akan diimplementasikan bersama oleh pihak yang tergabung dalam sistem aturan tersebut.

3. Pengamanan Nasional

Pengamanan metode ini adalah pengamanan yang ditetapkan oleh Regulator Nasional sebagai penyusun aturan nasional sistem aturan perbankan dan keuangan.

Dalam pelaksanaannya selain pihak yang bertanggung jawab, maka perangkat elektronis yang dipakai memerlukan pengamanan pula. Ada 3 perangkat sistem yang harus diberikan perhatian dalam pengamanannya.

1. Jaringan :

Untuk jaringan, maka ada 2 hal yang harus diberikan pengamanan :

a. Akses Jaringan

Akses jaringan dilakukan melalui saluran infrastruktur telekomunikasi

b. Enkripsi Lalu Lintas Jaringan

Enkripsi atau penyandian materi lalu lintas informasi yang melalui jaringan

2. Perangkat Keras :

Untuk perangkat keras pengamanan diterapkan melalui metode :

a. Toleransi Kesalahan (*Fault Tolerance*)
b. Tingkat toleransi mesin terhadap kerusakan yang terjadi pada perangkatnya
c. Penyiapan Cadangan (*Backup Recovery*)

d. Penyiapan cadangan/backup mesin untuk data yang diproses pada saat terjadi kerusakan pada mesin

e. Terminal Akses

3. Perangkat Lunak :

Untuk perangkat lunak pengamanan diterapkan dengan metode implementasi :

a. Pengamanan Sistem Operasi

b. Pemberian Kata Sandi / Password

Dengan pengaturan ini dapat diberikan hak akses kepada setiap petugas yang berwenang

c. Menu akses

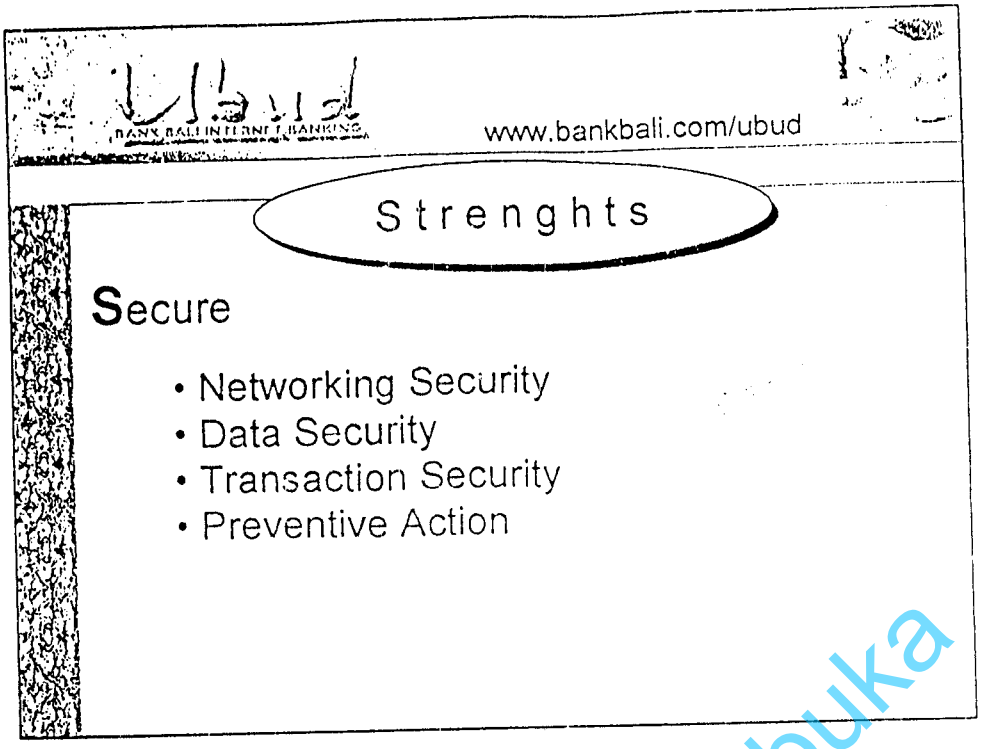
Menu-menu yang dapat diakses oleh setiap pemakai bergantung kepada kepentingan dan wewenangnya

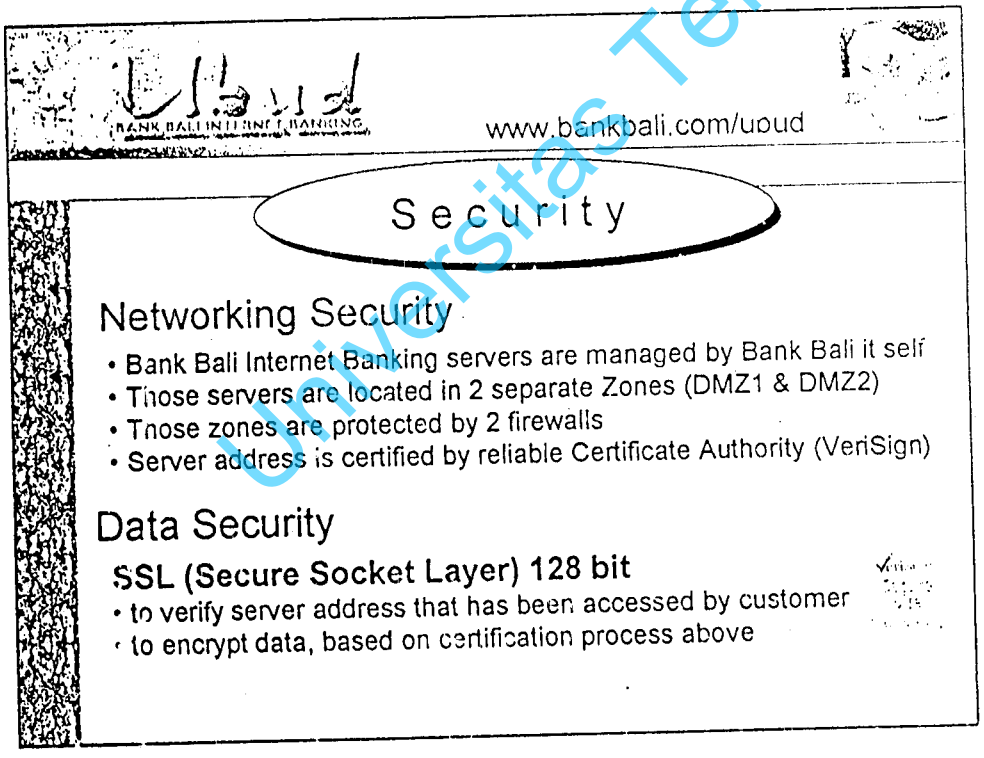
d. Enkripsi Data

Sama halnya dengan data yang dilalukan pada jaringan, maka data yang berada pada perangkat lunak maka untuk keamanannya dilakukan enkripsi/penyandian kode terlebih dahulu sehingga untuk membacanya harus dengan "kunci" tertentu.

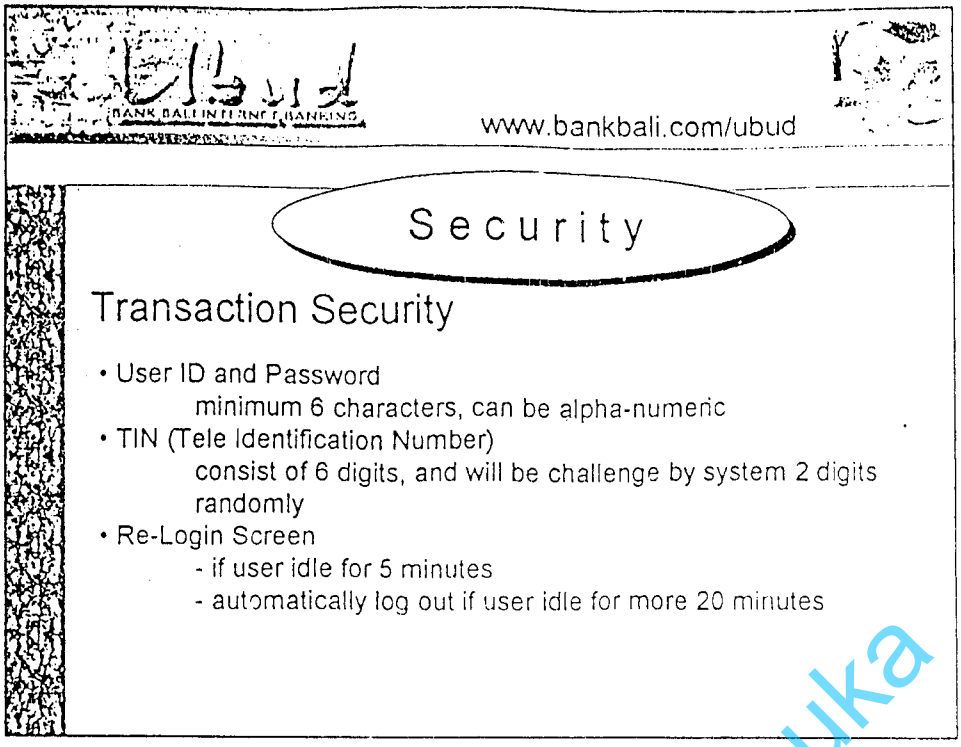
e. Manajemen Risiko

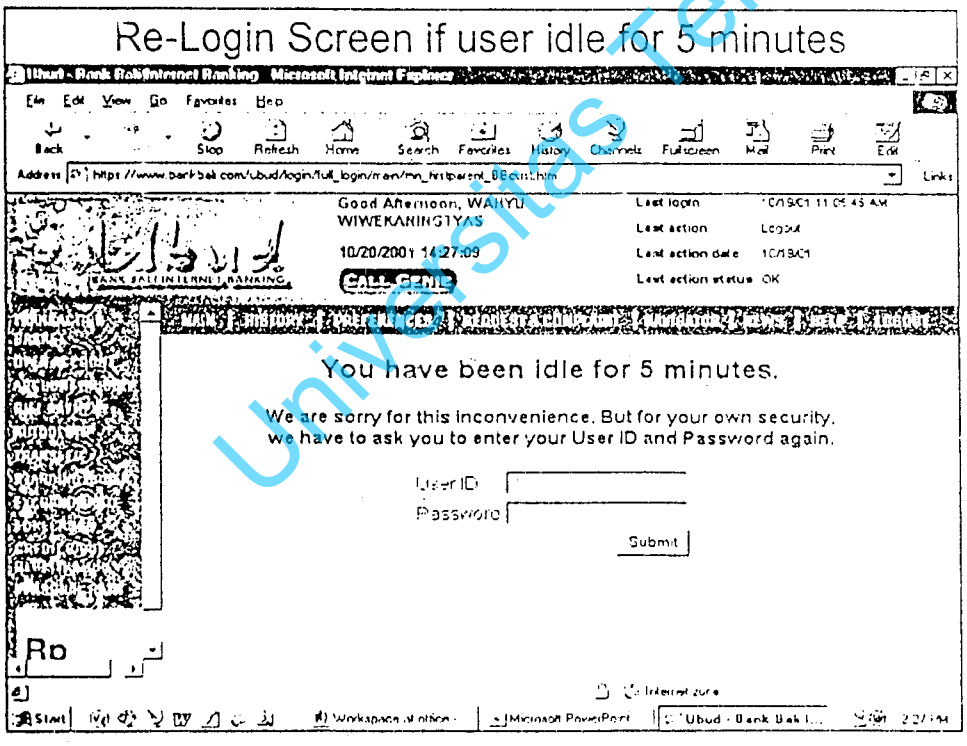
Dalam praktek, pada umumnya bank penyelenggara internet banking di Indonesia biasanya menggunakan sistem pengamanan berlapis seperti yang sudah disyaratkan yaitu SSL 128 bit, *firewall* dan disertifikasi oleh Verysign (Heru Sutadi, 2001). Sebagai contoh pengamanan yang dilakukan internet banking Bank Bali Ubud berikut ini (Gunawidjaja, 2001) :



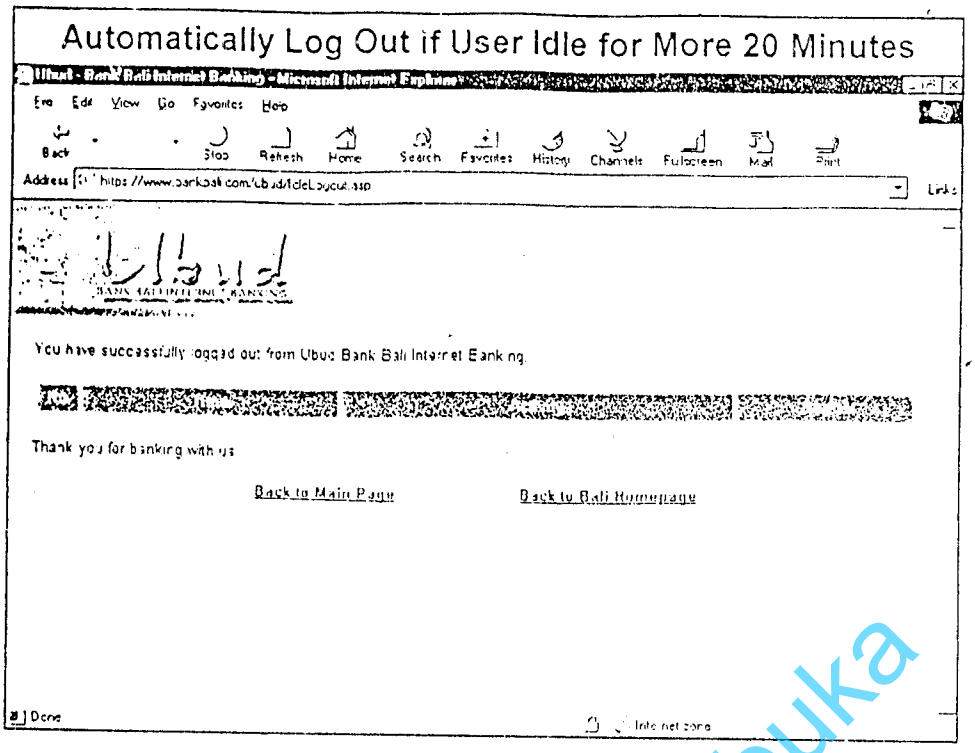


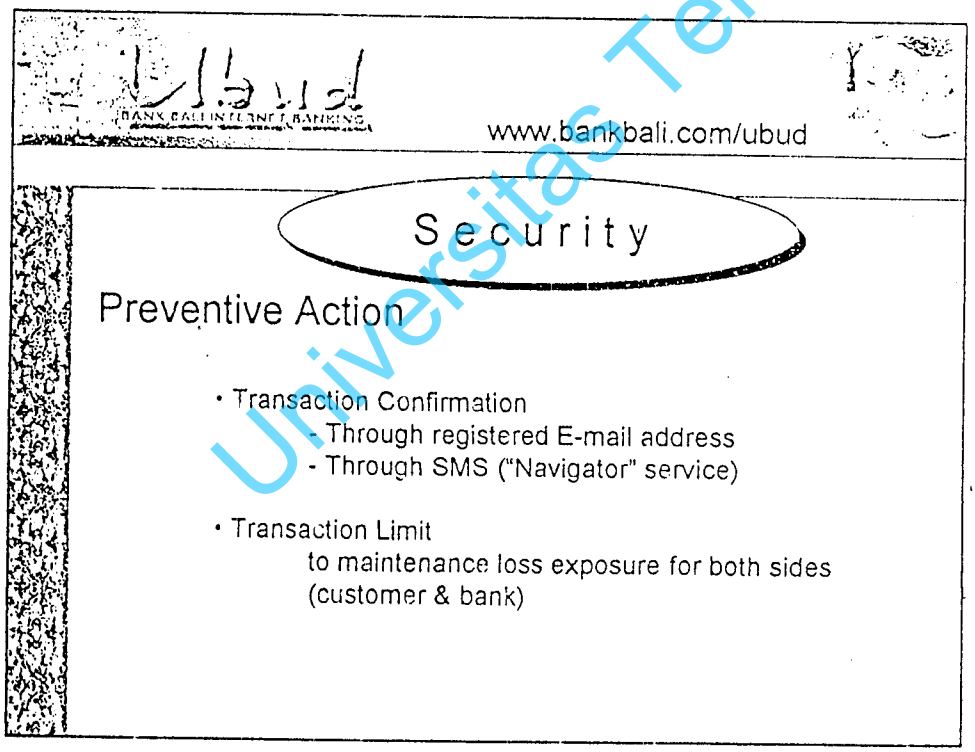
(Sumber : Gunawidjaja, 2001)





(Sumber : Gunawidjaja, 2001)





(Sumber : Gunawidjaja, 2001)

Standarisasi Perangkat Informasi

Sebagaimana diketahui, pelayanan perbankan berbasis internet merupakan jalur distribusi baru yang digunakan oleh kalangan perbankan di Indonesia dalam memenuhi tuntutan persaingan global perbankan di masa kini dan di masa depan. Oleh karena itu dunia perbankan memerlukan kesiapan dan standarisasi pemakaian peralatan pendukung bagi pelaksanaan aktivitas perbankan di masa datang,

Ada 2 kelompok besar yang harus dipersiapkan :

1. Perangkat Pengolah
2. Format Message Informasi

Untuk perangkat perbankan, yang harus dilakukan adalah sertifikasi perangkat yang kriteria sertifikasinya telah ditetapkan. Sertifikasi dapat dilakukan pada perangkat-perangkat :

1. EFT/POS = Electronic Fund Transfer/Point of Sales
2. ATM = Anjungan Tunai Mandiri
3. Mesin Debit/Credit Card
4. Mesin Smart Card

Sedangkan untuk format message, hendaknya dilakukan penyeragaman mengikuti standar yang telah diterapkan secara internasional dan telah diterakan seperti UN-EDIFACT.

C. PERATURAN PRAKTEK *INTERNET BANKING*

Sebagai suatu hal yang baru, maka Sistem Perbankan melalui Internet memerlukan suatu peraturan yang baku dan menyeluruh. Dengan hilangnya batas negara melalui media ini kembali muncul pertanyaan tentang regulasi dan peraturan yang sangat diperlukan bagi perbankan untuk prosedur yang berlaku bagi internet banking ini.

Banyak hal yang akan menjadi tidak pasti, dengan berlangsungnya sistem keuangan elektronis yang akan semakin berkembang dimasa datang ada beberapa permasalahan yang dapat diangkat yaitu :

1. Regulasi Prosedur Bank

   Meliputi penyiapan deposit, asuransi dsb.

2. Perlindungan Nasabah dan Pelanggan Bank

   Apakah perlindungan nasabah bank yang berlaku saat ini dapat diterapkan kepada pemakai sistem keuangan elektronis dan perlindungan apa lagi yang dapat diberikan bagi para nasabah dan pelanggan

3. Kerahasiaan Finansial

4. Komersial

   Siapakah yang bertanggung jawab terhadap hilangnya "uang" di dalam sistem elektronis, dan siapakah yang bertanggung jawab secara keseluruhan dalam sistem keuangan tersebut.

Meskipun sudah banyak bank di Indonesia yang menyelenggarakan Internet Banking, namun hingga kini belum terdapat pengaturan khusus yang mengatur kegiatan internet

banking yang dilakukan oleh perbankan Indonesia. Saat ini pengaturan untuk internet banking masih mengacu pada ketentuan Bank Indonesia yaitu SK Dir BI No. 27/164/KEP/DIR tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank yang mengatur tentang upaya pencegahan kemungkinan timbulnya risiko pelaksanaan teknologi sistem informasi serta langkah penanganannya.

Standarisasi Prosedur Perbankan

Didalam melakukan hubungan perbankan diperlukan suatu mekanisme tertentu baik di masa sekarang ataupun masa datang untuk suatu prosedur atau tata cara tertentu didalam melakukan hubungan perbankan.

Untuk selanjutnya maka pengelompokan sistem prosedur perbankan akan diarahkan pada 3 kelompok besar, yaitu :

1. Prosedur Internal Bank

   Hubungan internal di dalam suatu bank

2. Prosedur Antar Bank

   Hubungan antara suatu bank dengan bank lainnya, ini termasuk hubungan suatu bank dengan bank sentral

3. Prosedur Ekstra Bank

   Hubungan antara suatu bank dengan lembaga non-bank, baik individu, institusi maupun masyarakat banyak

Pada prosedur ekstra bank ini, prosedur dan persyaratan *Know Your Costumer* (KYC) yang diatur dengan Peraturan Bank Indonesia Nomor 3/23/PBI/2001 tentang Perubahan Atas Peraturan Bank Indonesia Nomor 3/10/PBI/2001 tentang Penerapan Prinsip Mengenal Nasabah dapat menjadi pedoman untuk mengatur hubungan antara bank dan nasabahnya.

Peraturan KYC mewajibkan setiap bank untuk membuat Pedoman Pelaksanaan Penerapan Prinsip Mengenal Nasabah yang mengacu pada SE BI No.3/29/DPNP tanggal 13 Desember 2001tentang Pedoman Standar Penerapan Prinsip Mengenal Nasabah, yang mengatur antara lain tentang Prosedur Penerimaan dan Identifikasi Nasabah serta Prosedur Pemantauan dan Pelaporannya, yaitu :

A. Prosedur Penerimaan dan Identifikasi Nasabah, meliputi :

1. Penerimaan Nasabah
2. Identifikasi dan Verifikasi (nasabah perorangan atau perusahaan)
3. Persetujuan Penerimaan Calon Nasabah

B. Prosedur Pemantauan dan Pelaporannya, meliputi :

1. Dokumentasi Profil Nasabah
2. Pemantauan Rekening dan Identifikasi Transaksi
3. Identifikasi Transaksi yang Mencurigakan

Dengan pengelompokan sistem prosedur perbankan yang diarahkan pada 3 kelompok besar seperti tersebut diatas, maka sistem prosedur perbankan yang ditetapkan akan dapat lebih antisipatif terhadap perkembangan teknologi yang semakin berkembang.

Berkaitan dengan itu yang harus diperhatikan untuk menetapkan standarisasi bagi sistem prosedur perbankan tersebut :

1. Akan menghilangnya batas dan kewenangan suatu negara dalam pengelolaan mata uang, ini diakibatkan adanya dunia keuangan akan mengarah ke pada pemakaian mata uang virtual (cyber money) yang akan meninggalkan "uang sesungguhnya" yang saat ini dikelola dan dimiliki oleh bank sentral.

2. Semakin rendahnya biaya yang diperlukan masyarakat untuk melakukan transaksi, ini mengakibatkan daya beli masyarakat yang semakin tinggi karena pasar yang akan mendekati mereka, bukan lagi masyarakat yang harus datang ke pasar. Ini merupakan tantangan perbankan untuk mengundang masyarakat tetap memanfaatkan jasa mereka terutama untuk menyimpan dananya di bank.

3. Perluasan pasar perbankan, dengan teknologi informasi dan telekomunikasi yang beragam segala macam aktivitas perbankan akan dapat ditawarkan dan dijual ke seluruh individu dan institusi di seluruh negara di dunia. Ini berakibat adanya kemungkinan bahwa suatu bank dapat beroperasi di seluruh dunia. Beroperasinya bank dari seluruh dunia di Indonesia tentu memerlukan suatu standarisasi tertentu yang berbeda dengan keadaan yang ada saat ini. Selain itu diperlukan pula suatu sistem prosedur perbankan dengan regulasi yang effisien sehingga tetap menarik bagi dunia perbankan untuk tetap beroperasi di Indonesia.

4. Kunci sukses bagi standarisasi yang diperlukan bagi sistem prosedur perbankan dimasa datang adalah transparansi, dilaksanakan tanpa pandang bulu, dan konsisten terhadap kebebasan individu sebagai pemakai jasa.

5. Penentuan prosedur kerja dalam rangka keterkaitan antara lembaga perbankan dengan lembaga yang terkait dengan keuangan individu nasabah perbankan, seperti Kantor Pajak memerlukan suatu pengaturan yang baku. Pengaturan tersebut bertujuan untuk mendukung suatu effisiensi nasional yang harus dilakukan dengan tanpa mengabaikan adanya hak nasabah.

D. PERLINDUNGAN NASABAH PENGGUNA *ELECTRONIC BANKING*

Pengaturan jasa *e-banking*, baik untuk jasa *electronic fund transfer* dan *internet banking*, secara umum belum dibuat oleh Bank Indonesia selaku otoritas pengawas sehingga syarat dan kondisi yang diterapkan antar bank berbeda-beda. Kondisi ini pada akhirnya cenderung menguntungkan bank dan merugikan nasabah. Berdasarkan hal tersebut, perlu segera dibuat peraturan tentang *e-banking* yang memberikan perlindungan kepada pengguna *e-banking*.

Untuk membuat peraturan tersebut, sebagai perbandingan (komparasi), dapat kita lihat pada the new Electronic Fund Transfer Code of Conduct (the Code) yang dikeluarkan oleh ASIC (Australian Securities and Investments Commission's) EFT Working Group in 2001, dimana dalam peraturan itu disebutkan antara lain :

1. The account holder has no liability for : (Para 5.2 of the Code)
   - losses that are caused by the fraudulent or negligent conduct of the employees or agents of the account institutions;
   - losses relate to forged, faulty, expired or cancelled access method;
   - losses that occure before the device or code has been received by the user, where a code or device is required for the user to use the access code; or

- losses that are caused by the same transaction being incorrectly debited more than once to the same account.

2. The account holder will also not liable in respect of any losses resulting from unauthorized transactions :
   - That occur after the account institution has been notified that any device forming part of the access method has been misused, lost or stolen or that the security codes forming part of the access method has been breached,
   - Where it is clear that the user has not contributed to such losses.
3. The account institutions liable in cases of system or equipment malfunction :
   - account institutions will be responsible to their users for loss caused by the failure of an institution system or institution equipment to complete a transaction accepted by an institution system or institution equipment in accordance with the user's instructions. (Para 6.1 of the Code)
   - prohibiting an account institution to deny any liability in the case of system malfunction. (Para 6.2 of the Code)

Menurut Maman H. Soemantri, untuk menimbulkan kepercayaan dan kenyamanan nasabah bertransaksi, hal yang perlu diterapkan oleh bank yaitu:

a. Sosialisasi nama *website* bank kepada nasabah serta *test and trial drive* kepada nasabah.

b. Perbankan diharapkan menyusun privacy policy untuk melindungi data nasabah.

c. Sebelum menggunakan layanan *internet banking* bank harus memastikan nasabah memahami *terms and condition,* risiko transaksi serta *privacy policy* bank.

d. Bank harus memberikan *client* charter/garansi untuk melaksanakan operasional *internet banking* yang aman.

BAB IV. KESIMPULAN DAN SARAN

A. KESIMPULAN

Dengan bertambahnya ragam pelayanan pada nasabah/pengguna dengan teknologi pelayanan perbankan yang semakin maju, ketergantungan dunia perbankan pada dunia telekomunikasi dan sistem informasi akan semakin meningkat. Oleh karena itu, tidak hanya prosedur perbankan yang harus ditentukan dan didefinisikan, tetapi prosedur dan standarisasi perangkat informasi perbankan pun harus diperhatikan.

B. SARAN

Dalam pengaturan internet banking, hukum seharusnya *technology neutral* sehingga adanya perubahan teknologi tidak harus mengubah hukum yang ada. Hukum yang mengatur *e-banking* harus dapat menimbulkan kepercayaan dan kenyamanan nasabah dalam bertransaksi.

DAFTAR PUSTAKA / BACAAN ACUAN

Budi Rahardjo, *Aspek Teknologi dan Keamanan Dalam Internet Banking,* Seminar *Internet Banking, Implementasi dan Tantangannya ke Depan,* Direktorat Penelitian dan Pengaturan Perbankan-Bank Indonesia, Jakarta 13 Agustus 2001

Gunawidjaja, *Bank Bali Internet Banking,* Seminar *Kebutuhan Legal Audit Terhadap Penerapan Teknologi Sistem Informasi Perbankan Serta Kaitannya Dengan Penerapan Internet Banking*, LKHT-UI, Jakarta 31 Oktober 2001.

Heru Sutadi, *Kejahatan Perbankan Lewat Internet*, Kompas Cyber 8 Juli 2001

I Made Wiryana dan Tedi, Heriyanto, *Resiko Internet Banking Telah Tampak,* (http://www.tedi-h.com/papers/I-banking.html)

Kusumaningtuti S.S, *Legal Audit Terhadap Penerapan Teknologi Sistem Informasi Perbankan Serta Kaitannya Dengan Penerapan Internet Banking*, Seminar *Kebutuhan Legal Audit Terhadap Penerapan Teknologi Sistem Informasi Perbankan Serta Kaitannya Dengan Penerapan Internet Banking*, LKHT-UI, Jakarta 31 Oktober 2001.

Maman H.Soemantri, *Urgensi Cyber Law Dalam Perkembangan Internet Banking di Indonesia*, Seminar Kebutuhan Legal Audit Terhadap Penerapan Teknologi Sistem Informasi Perbankan Serta Kaitannya Dengan Penerapan Internet Banking, LKHT-UI, Jakarta 31 Oktober 2001.

Sri Hariningsih, *Keabsahan Transaksi Elektronik dan Aspek Hukum Pembuktian Terhadap Data Elektronik di Indonesia*, Seminar Kebutuhan Legal Audit Terhadap Penerapan Teknologi Sistem Informasi Perbankan Serta Kaitannya Dengan Penerapan Internet Banking, LKHT-UI, Jakarta 31 Oktober 2001.

Syahril Sabirin, *Urgensi Regulasi Dalam Internet Banking*, *Keynote Speaker* Seminar Sehari *"Aspek Hukum Internet Banking Dalam Kerangka Hukum Teknologi Informasi (Cyber Law)"*, Pusat Studi *Cyber Law* FH-UNPAD bekerjasama dengan Koperasi Karyawan Bank Bali Cabang Bandung, Bandung 13 Juli 2001.

Taufik Akbar,dkk.,editor, *Nusantara 21 Aplikasi Perbankan dan Keuangan*, Jakarta : Yayasan Litbang Telekomunikasi Informatika, 1998.

.... *Distribution of Liability in Internet Banking : Law and Practice*, Workshop Materials in Internet Banking Workshop, Center for Regulatory Research, Jakarta 18 September 2002

Peraturan Bank Indonesia Nomor 3/23/PBI/2001 tentang Perubahan Atas Peraturan Bank Indonesia Nomor 3/10/PBI/2001 tentang Penerapan Prinsip Mengenal Nasabah

SE BI No.3/29/DPNP tanggal 13 Desember 2001tentang Pedoman Standar Penerapan Prinsip Mengenal Nasabah

Kompas Cyber, 26 April 2002

Suara Merdeka, 16 Nopember 2002