Arsitektur Internet Banking Yang Terpercaya: *Trusted Internet Banking Architecture*

Budi Rahardjo[1]
INDOCISC.com[2]
budi@indocisc.com
2002

Daftar Isi

1 Persyaratan Bisnis 2
2 Persyaratan Keamanan 3
2.1 Confidentiality 4
2.2 Integrity 4
2.3 Authentication 4
2.4 Non-repudiation 5
2.5 Availability 5
3 Implementasi Sistem 5
3.6 Front-end 6
3.7 Back-end 7
4 Penutup 8
5 Bahan Bacaan 8

Perkembangan teknologi informasi, telekomunikasi, dan Internet menyebabkan mulai munculnya aplikasi bisnis yang berbasis Internet. Salah satu aplikasi yang mulai mendapat perhatian adalah Internet Banking atau sering juga disebut *e-Banking*[3]. Beberapa statistik menunjukkan naiknya jumlah pelaku e-Banking di dunia. Di Indonesia sudah ada beberapa pelaku Internet Banking. Salah satu pelaku yang cukup dikenal di masyarakat adalah layanan "KlikBCA"[4] dari BCA.

Salah satu aspek yang sangat penting dalam layanan perbankan adalah aspek keamanan (*security*). Sayangnya masalah keamanan ini seringkali terabaikan (baik secara teknis dan non-teknis) sehingga terjadi beberapa masalah. Di Indonesia sudah ada beberapa berita mengenai orang yang merasa uangnya dicuri melalui transaksi Internet Banking. Adanya situs "plesetan" (*typosquatter*) kilkbca.com yang

[1] Budi Rahardjo merupakan Chief Technology Officer dari PT INDOCISC, peneliti di Pusat Penelitian Antar Universitas Bidang Mikroelektronika (PPAUME) Institut Teknologi Bandung.

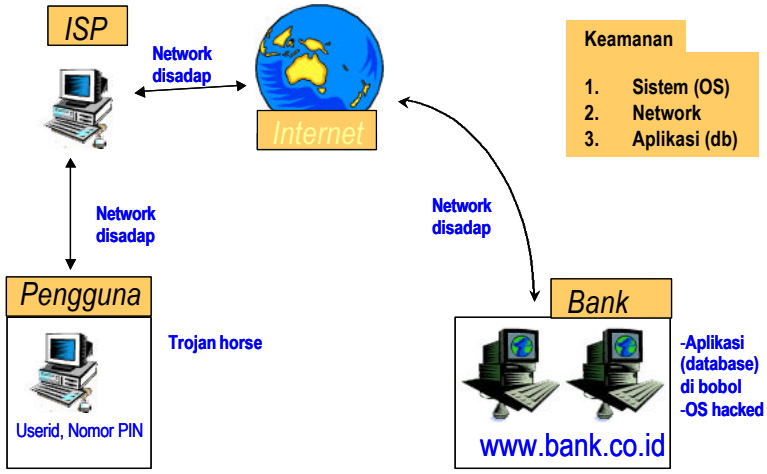
[2] PT INDOCISC merupakan sebuah perusahaan yang bergerak dalam bidang jasa keamanan (*security*) dari sistem informasi, termasuk network security. Informasi lengkap ada pada situs http://www.indocisc.com

[3] Untuk selanjutnya dalam white paper ini terminologi "e-banking" dianggap sama dengan "Internet Banking".

[4] Lihat situs http://www.klikbca.com

bukan milik BCA akan tetapi dibuat menyerupai klikbca.com juga menjadi fakta yang menodai Internet Banking di Indonesia. Jika masalah ini tidak diatasi, maka kepercayaan masyarakat akan amannya transaksi Internet Banking menjadi luntur dan menyebabkan layanan ini dihindari.

Masalah keamanan merupakan salah satu topik yang cukup kompleks. Pembahasan pada white paper ini tidak dapat secara menyeluruh dan hanya difokuskan kepada aplikasi Internet Banking. Pembahasan secara rinci mengenai keamanan sistem informasi dapat dilihat pada buku referensi yang terdapat pada bagian akhir dari *white paper* ini. Secara umum potensi lubang keamanan (security hole) yang dapat dieksploitasi dalam Internet Banking dapat dilihat pada gambar berikut:



Gambar 1. Potensi sumber lubang keamanan dalam Internet Banking

Pada gambar di atas terlihat bahwa keamanan tidak hanya bergantung kepada jaringan (network) saja, melainkan juga bergantung kepada operating system (OS) dan aplikasi (database). Pengamanan yang terfokus pada network saja (misalnya hanya menggunakan SSL) tanpa melihat secara keseluruhan akan berakibat fatal.

1 Persyaratan Bisnis

Persayaratan bisnis dari Internet Banking antara lain:

- aplikasi mudah digunakan;
- layanan dapat dijangkau dari mana saja;
- murah;
- aman;
- dan dapat diandalkan (*reliable*)

Beberapa implementasi dari electronic banking sebelum Internet populer adalah dengan mengembangkan aplikasi sendiri. Namun pendekatan ini mulai ditinggalkan karena penyedia jasa harus menyediakan berbagai versi dari program aplikasi itu, misalnya untuk versi Microsoft Windows, Macintosh, dan sistem operasi yang populer lainnya. Agar mudah digunakan, akhirnya banyak pelaku Internet Banking yang memilih menggunakan web browser.

Aspek kedua, layanan dapat dijangkau dari mana saja. Aspek ini dapat dipenuhi dengan menggunakan Internet sebagai jaringan penghubung. Internet sudah dapat diakses darimana saja di dunia.

Aspek berikutnya adalah murahnya biaya untuk mengakses Internet Banking. Penggunaan Internet menyebabkan layanan bisa menjadi murah.

Aspek pengamanan dapat dilakukan dengan menggunakan teknologi kriptografi seperti penggunaan enkripsi dengan menggunakan SSL (Secure Socket Layer). Pada prinsipnya dia mengacak dan menyandikan data sehingga sulit disadap oleh orang yang tidak berhak. Pengamanan lain adalah penggunaan VPN (Virtual Private Network) untuk menghubungkan kantor pusat bank dengan kantor cabang.

Aspek-aspek di atas merupakan aspek yang dilihat dari sudut pandang pengguna (nasabah). Ada aspek lain yang dilihat dari kacamata penyedia jasa (bank), antara lain:

- **Mudah meluncurkan aplikasi / produk / servis lain**. Saat ini mungkin bank baru memikirkan Internet Banking. Akan tetapi di kemudian hari akan muncul layanan mobile banking, TV banking, dan berbagai layanan baru lainnya yang belum terbayang pada saat ini. Sistem yang ada harus dapat meluncurkan layanan ini dengan cepat. Time to market merupakan kunci utama dalam era digital ini.
- **Scalability, baik dalam ukuran maupun dalam kecepatan**. Sistem yang ada harus dapat melayani nasabah dalam jumlah kecil, misalnya ribuan orang, sampai ke nasabah dalam jumlah besar, misalnya belasan juta orang. Seringkali sistem yang dikembangkan hanya dapat bekerja untuk jumlah nasabah yang sedikit sehingga ketika servis menjadi populer dan nasabah mulai banyak menggunakan servis tersebut maka servis menjadi sangat lambat.
- **Dapat mengakomodasi platform / sistem yang berbeda-beda (heterogen)**. Multi-channel access merupakan paradigma yang harus didukung. Pada masa yang akan datang, layanan diharapkan dapat diakses dari berbagai platform; mulai dari datang ke counter, diteruskan dengan akses lewat Internet, dan kemudian diselesaikan melalui handphone.
- **Memiliki sifat resilency, tahan bantingan dan cepat kembali ke kondisi semula jika terjadi masalah**. Musibah tidak dapat diprediksi. Banjir, kebakaran, kerusuhan, dan berbagai hal lainnya dapat menyebabkan terhentinya layanan. Servis Banking (termasuk Internet Banking) harus dapat kembali menjalankan layanan dalam waktu sesingkat mungkin.
- **Manageable**. Sistem yang ada harus dapat dikelola dengan baik. Meningkatnya variasi dan kompleksitas dari layanan sering menyebabkan kompleksitas di sisi sistem yang mengimplementasikan layanan tersebut. Untuk itu sistem Internet Banking yang ada harus dapat dikelola (manageable). Jika tidak, sistem akan menjadi kacau balau dan tidak terkendali.

2 Persyaratan Keamanan

Aspek keamanan yang harus dijaga dari Internet Banking adalah:

- *Confidentiality*: dimana data-data harus diamankan dari penyadapan
- *Integrity*: data tidak boleh diubah tanpa ijin dari yang berhak
- *Authentication*: untuk meyakinkan identitas nasabah **dan** identitas dari situs web

- *Non-repudiation*: bahwa nasabah tidak dapat menyangkal telah melakukan transaksi
- *Availability*: terkait dengan ketersediaan layanan, termasuk up-time dari situs web

Aspek-aspek di atas harus dapat diberikan dalam implementasi dari Internet Banking. Berikut ini sedikit penjabaran dari aspek-aspek di atas.

2.1 *Confidentiality*

Aspek *confidentiality* memberi jaminan bahwa data-data tidak dapat disadap oleh pihak-pihak yang tidak berwenang. Serangan terhadap aspek ini adalah penyadapan nama account dan PIN dari pengguna Internet Banking. Penyadapan dapat dilakukan pada sisi terminal (komputer) yang digunakan oleh nasabah atau pada jaringan (network) yang mengantarkan data dari sisi nasabah ke penyedia jasa Internet Banking. Penyadapan di sisi komputer dapat dilakukan dengan memasang program *keylogger* yang dapat mencatat kunci yang diketikkan oleh pengguna. Penggunaan *keylogger* ini tidak terpengaruh oleh pengamanan di sisi jaringan karena apa yang diketikkan oleh nasabah (sebelum terenkripsi) tercatat dalam sebuah berkas.

Penyadapan di sisi jaringan dapat dilakukan dengan memasang program sniffer yang dapat menyadap data-data yang dikirimkan melalui jaringan Internet. Pengamanan di sisi network dilakukan dengan menggunakan enkripsi. Teknologi yang umum digunakan adalah *Secure Socket Layer* (SSL) dengan panjang kunci 128 bit.

Pengamanan di sisi komputer yang digunakan nasabah sedikit lebih kompleks. Hal ini disebabkan banyaknya kombinasi dari lingkungan nasabah. Jika nasabah mengakses Internet Banking dari tempat yang dia tidak kenal atau yang meragukan integritasnya seperti misalnya warnet yang tidak jelas, maka kemungkinan penyadapan di sisi terminal dapat terjadi. Untuk itu perlu disosialisasikan untuk memperhatikan tempat dimana nasabah mengakses Internet Banking. Penggunaan key yang berubah-ubah pada setiap sesi transaksi (misalnya dengan menggunakan token generator) dapat menolong. Namun hal ini sering menimbulkan ketidaknyamanan.

Sisi back-end dari bank sendiri harus diamankan dengan menggunakan *Virtual Private Network* (VPN) antara kantor pusat dan kantor cabang. Hal ini dilakukan untuk menghindari adanya fraud yang dilakukan dari dalam (internal).

2.2 *Integrity*

Aspek integrity menjamin integritas data, dimana data tidak boleh berubah atau diubah oleh pihak-pihak yang tidak berwenang. Salah satu cara untuk memproteksi hal ini adalah dengan menggunakan *checksum*, *signature*, atau *certificate*. Mekanisme signature akan dapat mendeteksi adanya perubahan terhadap data.

Selain pendeteksian (dengan menggunakan *checksum*, misalnya) pengamanan lain yang dapat dilakukan adalah dengan menggunakan mekanisme *logging* (pencatatan) yang ekstensif sehingga jika terjadi masalah dapat dilakukan proses mundur (rollback).

2.3 *Authentication*

Authentication digunakan untuk meyakinkan orang yang mengakses servis dan juga server (web) yang memberikan servis. Mekanisme yang umum digunakan untuk melakukan authentication di sisi pengguna biasanya terkait dengan:

- Sesuatu yang dimiliki (misalnya kartu ATM, *chipcard*)
- Sesuatu yang diketahui (misalnya *userid*, *password, PIN, TIN*)
- Sesuatu yang menjadi bagian dari kita (misalnya sidik jari, *iris* mata)

Salah satu kesulitan melakukan authentication adalah biasanya kita hanya menggunakan userid/account number dan password/PIN. Keduanya hanya mencakup satu hal saja (yang diketahui) dan mudah disadap. Pembahasan cara pengamanan hal ini ada pada bagian lain.

Sementara itu mekanisme untuk menunjukkan keaslian server (situs) adalah dengan digital certificate. Sering kali hal ini terlupakan dan sudah terjadi kasus di Indonesia dengan situs palsu "kilkbca.com". Situs palsu akan memiliki sertifikat yang berbeda dengan situs Internet Banking yang asli.

2.4 *Non-repudiation*

Aspek nonrepudiation menjamin bahwa jika nasabah melakukan transaksi maka dia tidak dapat menolak telah melakukan transaksi. Hal ini dilakukan dengan menggunakan digital signature yang diberikan oleh kripto kunci publik (*public key cryptosystem*). Mekanisme konfirmasi (misal melalui telepon) juga merupakan salah satu cara untuk mengurangi kasus.

Penggunaan logging yang ekstensif juga dapat mendeteksi adanya masalah. Seringkali logging tidak dilakukan secara ekstensif sehingga menyulitkan pelacakan jika terjadi masalah. (Akses dari nomor IP berapa? Terminal yang mana? Jam berapa? Apa saja yang dilakukan?)

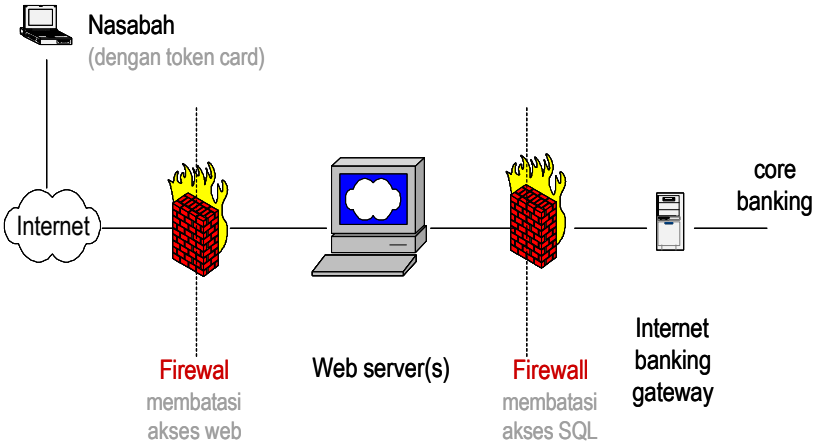
2.5 *Availability*

Aspek availability difokuskan kepada ketersediaan layanan. Jika sebuah bank menggelar layanan Internet Banking dan kemudian tidak dapat menyediakan layanan tersebut ketika dibutuhkan oleh nasabah, maka nasabah akan mempertanyakan keandalannya dan meninggalkan layanan tersebut. Bahkan dapat dimungkinkan nasabah akan pindah ke bank yang dapat memberikan layanan lebih baik. Serangan terhadap availability dikenal dengan istilah *Denial of Service* (DoS) *attack*. Sayangnya serangan seperti ini mudah dilakukan di Internet dikarenakan teknologi yang ada saat ini masih menggunakan IP (Internet Protocol) versi 4.

Mekanisme pengamanan untuk menjaga ketersediaan layanan antara lain menggunakan backup sites, DoS filter, *Intrusion Detection System* (IDS), network monitoring, *Disaster Recovery Plan* (DRP), *Business Process Resumption*. Istilah-istilah ini memang sering membingungkan (dan menakutkan). Mereka adalah teknik dan mekanisme untuk meningkatkan keandalan.

3 Implementasi Sistem

Arsitektur dari sistem Internet Banking yang aman menggunakan filosofi pengamanan berlapis. Dalam hal ini sistem dibagi menjadi beberapa level (tier). Secara garis besar, sistem dapat dibagi menjadi dua bagian: *front-end* (yang berhubungan dengan nasabah) dan *back-end* (yang berhubungan dengan bank). Kedua bagian ini biasanya dipisahkan dengan firewall (bisa sebuah firewall atau beberapa firewall jika dibutuhkan keandalan dan kinerja yang sangat tinggi).



Gambar 2. Topologi Internet Banking dengan pengamanan yang berlapis

3.6 *Front-end*

Bagian front-end merupakan bagian yang langsung berhubungan dengan nasabah. Melihat persyaratan yang ditelah diungkapkan pada bagian terdahulu, bagian ini menggunakan web browser sebagai *user interface*.

Beberapa topik yang menarik untuk dibahas pada bagian front-end adalah disain dari *interface* yang memudahkan bagi pengguna. Perlu diingat bahwa nasabah memiliki latar belakang dan mekanisme akses yang beragam. Ada nasabah yang melakukan akses dari kantor dengan komputer desktop yang high-end. Sementara itu ada nasabah yang menggunakan komputer biasa dengan hubungan *dialup*. Untuk itu disain jangan menggunakan grafik yang berlebihan (misalnya).

Masalah pengamanan di bagian front-end juga sering terlupakan. Kasus-kasus Internet Banking umumnya terjadi di sisi ini. Nasabah misalnya menggunakan akses dari terminal di warnet yang sudah dipasangi alat penyadap kunci yang kita ketikkan (dikenal dengan istilah *key logger*). Akibat dari ulah ini maka penyadap dapat mengetahui account dan nomor PIN nasabah. Untuk itu perlu dilakukan sosialisasi terhadap pengguna untuk mengakses layanan Internet Banking melalui fasilitas yang dikenal aman.

Penggunaan *token generator* atau *cryptocard* yang menghasilkan password yang berubah-ubah setiap sesinya merupakan salah satu usaha untuk meningkatkan pengamanan. Bentuk dari token generator ini ada yang berupa kalkulator sampai ke bentuk gantungan kunci. Namun pendekatan ini menjadi mahal karena harus memberikan token generator kepada setiap nasabah. Jika jumlah nasabah adalah jutaan, maka hal ini menjadi penghambat utama. Penghambat lain adalah jika nasabah memiliki beberapa account di bank yang berbeda-beda maka dia harus memiliki token generator yang berbeda-beda sehingga tidak nyaman (bahkan tidak mungkin) dibawa pada saat yang bersamaan. Maukah anda mengantongi 3 atau 4 token generator dalam bentuk kalkulator? Tentunya tidak! Selain itu penggunaan token generator ini sering membingungkan bagi nasabah dan tidak nyaman.

[Catatan: Di INDOCISC kami sedang mengembangkan beberapa ide untuk meningkatkan keamanan di sisi nasabah ini.]

Penanganan masalah di sisi nasabah sering terkait dengan penyedia jasa akses seperti Internet Service Provider (ISP). Banyak penyedia jasa yang belum dapat diajak bekerja sama jika terjadi masalah. Sebagai contoh, jika terjadi transaksi fiktif dan dilacak sampai ke sebuah ISP, sejauhmana ISP akan membantu pihak bank

untuk melakukan pengusutan? Seringkali mereka tidak mau karena kesibukan mereka dan tidak adanya keuntungan secara finansial (bahkan harus keluar biaya) untuk melakukan hal tersebut. Hal ini perlu mendapat perhatian kita bersama.

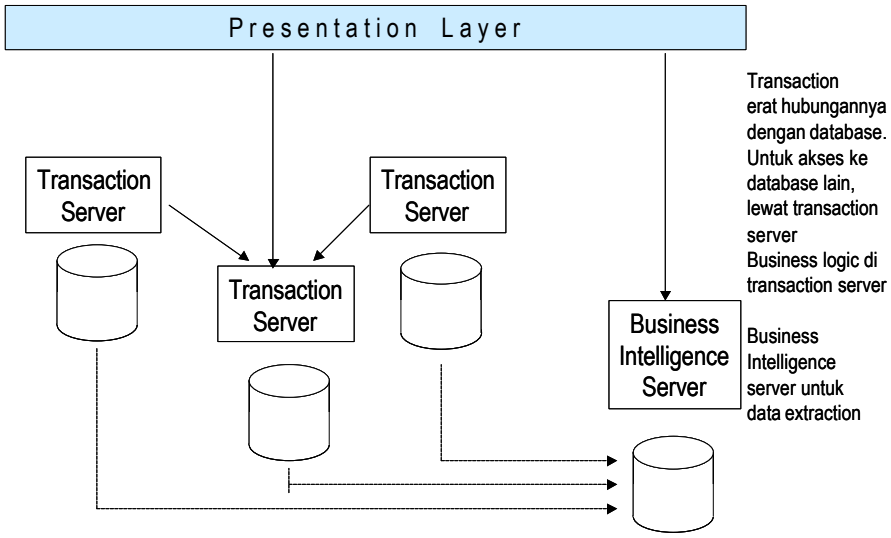
3.7 *Back-end*

Sisi back-end (dapur) merupakan hal yang terpenting. Implementasi di sisi back-end harus dapat memenuhi aspek-aspek yang disyaratkan (secara bisnis maupun secara teknis). Dilihat dari sisi arsitektur di back-end, terlihat adanya trend untuk menggunakan middleware. Sistem dipisahkan menjadi tiga aspek:

- Presentation layer
- Transaction layer
- Data(base) layer

Pemisahan di atas dilakukan untuk memudahkan implementasi dan mempercepat *deployment* aplikasi baru. Pendekatan *layering* ini mirip dengan layering di sisi network (*OSI 7 layer*) yang terbukti ampuh dalam dunia Internet.

Implementasi yang ada saat ini sering sepotong-sepotong sehingga menyulitkan pengelolaan (management). Data tersebar di berbagai database yang terkait dengan aplikasi tertentu sehingga menyulitkan untuk mengintegrasikan data-data. Implementasi yang terpadu (*integrated*) akan memudahkan perusahaan di kemudian hari.



Gambar 3. Transaction & database servers [Britton, 2001]

Pengamanan di sisi backend harus berlapis-lapis sehingga jika terjadi kebocoran tidak semua sistem menjadi kolaps. Perlu diingat pada bagian back-end ini pengamanan juga harus meliputi pengamanan kemungkinan terjadinya fraud yang dilakukan oleh orang dalam.

Pengamanan biasanya menggunakan komponen standar seperti:

- Firewall: sebagai pagar untuk menghadang usaha untuk masuk ke sistem. Firewall juga bersifat sebagai *deterant* bagi orang yang ingin coba-coba.
- Intrusion Detection System (IDS): sebagai pendeteksi adanya aktivitas yang sudah terjadi/dilanggar.

- Network monitoring tools: sebagai usaha untuk mengamati kejahatan yang dilakukan melalui jaringan dikarenakan layanan Internet Banking dapat dilakukan dari mana saja melalui network.
- Log processor & analysis: untuk melakukan pendeteksi dan analisa terhadap kegiatan yang terjadi di sistem. Seringkali hal ini tidak dilakukan.

Selain hal-hal di atas, masih ada hal lain seperti mekanisme "incident handling", organisasi yang menanganinya. (Apakah anda sudah memiliki *incident response team* di tempat anda? Jika sudah ada apakah letaknya di bawah IT atau operation atau internal audit atau unit tersendiri?)

4 Penutup

Dokumen ini membahas secara sepintas tentang arsitektur Internet Banking yang terpercaya. Sengaja kami menggunakan kata "terpercaya" karena hal ini yang lebih penting dibandingkan dengan memiliki sistem yang lebih aman (secara teknis) namun tidak dipercaya oleh nasabahnya.

Beberapa mekanisme implementasi membutuhkan adanya Public Key Infrastructure (PKI). Namun sayangnya hal ini belum tersedia di Indonesia. Sebagai contoh, untuk digital certificate kita masih menggunakan layanan Verisign yang berada di Amerika. Sementara itu status hukum dari digital signature di Indonesia masih dalam proses dan diharapkan dapat selesai sesegera mungkin.

Untuk pembahasan yang lebih rinci, INDOCISC memberikan layanan konsultasi untuk Internet Banking dan hal-hal lain yang berhubungan dengan masalah security.

5 Bahan Bacaan

1. Budi Rahardjo, "Keamanan Sistem Informasi Berbasis Internet," PT Insan Infonesia & PT INDOCISC, *downloadable book* yang dapat diperoleh dari http://budi.insan.co.id
2. S. Soundararajan, dan Debanjan Dey, "Architecting e-Banking High Assurance Security Solution," Infosys.
3. Chris Britton, "IT Architecture and Middleware: strategies for building large integrated systems," Addison Wesley, 2001