Penerapan Kriptografi dalam Pengamanan Transaksi Internet Banking

Humasak Simanjuntak[1] dan Marojahan Sigiro[2]

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : humasak@students.if.itb.ac.id[1], marojahan@students.if.itb.ac.id[2]

Abstrak

Perkembangan teknologi internet menyebabkan banyaknya sistem yang dikembangkan dengan menggunakan komunikasi melalui internet. Internet Banking adalah sebuah sistem perbankan yang menjalankan operasinya dengan menggunakan komunikasi melalui internet. Dalam melakukan komunikasi melalui internet, banyak resiko keamanan yang harus dihadapi apalagi berkaitan dengan transaksi yang ada di bank. Salah satu solusi yang diberikan untuk menangani masalah keamanan ini adalah penerapan kriptografi dalam Internet Banking. Penerapan kriptografi ini meliputi enkripsi pesan dan autentikasi nasabah (*customer*) dan bank yang melakukan transaksi. Dengan penerapan kriptografi ini, diharapkan terbentuknya transaksi yang aman dalam sistem internet banking. Makalah ini akan menjelaskan lebih detail mengenai penerapan kriptografi dalam proses autentikasi Internet banking

***Kata kunci** : Internet Banking, Kriptografi, Autentikasi internet-banking*

1. Pendahuluan

Definisi Internet Banking mengacu kepada sistem yang memampukan *customer* mengakses accountnya dan informasi yang umum pada produk maupun pelayanan melalui PC atau device yang lain. Dalam hal ini, produk dan *service* yang diberikan oleh internet banking dapat berupa penjualan produk kepada *customer* seperti menjual dan menggadaikan produk untuk konsumen. Pada akhirnya, produk dan *service* yang diperoleh melalui internet banking mencerminkan produk dan *service* yang ditawarkan melalui saluran penjualan oleh bank lain. Beberapa contoh produk dan *service* yang disediakan pada internet banking adalah :

1. Pengaturan keuangan (Cash).
2. Informasi saldo.
3. Transfer dana.
4. Pembayaran bill.
5. Transaksi ACH (*Automated Clearing house*).
6. Aplikasi peminjaman.
7. Aktivitas untuk melakukan penanaman modal (investasi)

Pelayanan internet banking termasuk menyediakan akses internet sebagai sebuah *Internet Service Provider* (ISP). Dimana, sebuah bank, menyediakan *service* yang dimilikinya kepada *customer* melalui koneksi internet ke sistem dari bank tersebut. Dahulu, sistem komputer yang dibuat sebagai sebuah operasi sistem informasi jarang diperhatikan oleh *customer*. Pada saat ini, web site, e-mail dan sistem pembayaran secara elektronik merupakan suatu cara yang penting bagi bank

untuk mencapai *customer*nya. Beberapa tahun yang lalu, *online banking* dilakukan melalui *dial-in* atau koneksi TV kabel. Sistem ini membatasi *customer* karena area yang dapat dijangkaunya terbatas. Dengan perkembangan Internet yang pesan, *customer* dapat menggunakan teknologi ini dimana saja untuk mengakses jaringan dari bank. Internet sebagai sebuah teknologi membuat produk dan *service* bank tersedia kepada lebih banyak *customer* tanpa membatasi daerah geografik.

1.1 Resiko

Dengan penerapan internet banking, resiko-resiko yang dihadapi suatu bank dalam operasinya juga makin besar. Resiko ini meliputi resiko keamanan maupun resiko yang berkaitan dengan pendapatan atau kegiatan utama bank. Beberapa resiko yang harus ditangani (diawasi) oleh pihak bank yaitu :

1. Resiko keamanan
   Dalam hal ini pihak bank harus memperhitungkan semua aspek keamanan yang mungkin terjadi pada transaksi ada pada internet banking. Semakin berkembangnya teknologi internet menyebabkan resiko keamanan yang terjadi semakin besar. Hal ini merupakan resiko utama dalam penerapan internet banking. Bayangkan bila seseorang dapat melakukan transaksi dengan menggunakan *account number* orang lain, sedangkan pemilik account tersebut menyangkal adanya transaksi tersebut, atau seseorang yang masuk ke sebuah situs bank yang salah yang menyediakan sistem internet banking. Hal ini akan menyebabkan ketidaknyamanan bagi customer untuk menggunakan pelayanan yang ada pada bank karena tidak terjaminnya keamanan.
2. Resiko yang berkaitan dengan pendapatan/kegiatan utama perusahaan.
   Resiko ini meliputi resiko kredit, liquiditas, resiko harga, resiko transaksi, strategi, dan resiko strategi yang digunakan oleh bank dalam penerapan internet banking.

2. Isu dalam Internet Banking

Resiko-resiko yang timbul dalam penerapan internet banking menyebabkan adanya isu yang berkembang saat ini dalam penanganan resiko maupun pemeliharaan keamanan pada internet banking. Isu tersebut meliputi *security*, autentikasi, *Trust*, *Nonrepudiation*, dan *Privacy*.

2.1 *Security*

Keamanan merupakan isu yang sangat penting pada penerapan internet banking. Setiap bank seharusnya menyediakan sebuah level keamanan baik logik maupun fisik yang memiliki toleransi terhadap sensitivitas informasi bank

Beberapa bank mengijinkan akses *dial-in* secara langsung kepada sistem mereka melalui sebuah private network ketika yang lain menyediakan akses melalui internet. Meskipun publik dapat mengakses Internet, namun secara umum kurang aman untuk melakukan transaksi. Contoh: *Hardware* atau *software* dari ”sniffer” dapat memperoleh password, *account number*, nomor kartu kredit dan lain-lain tanpa akses yang legal. Oleh karena itu, keamanan melalui elektronik akses harus dilindungi. Sistem yang ada harus mampu mencegah, mendeteksi dan mengatur dengar benar untuk menjamin integritas dari jaringan dan informasi ditangani. Contoh: penggunaan firewall.

2.2 Autentikasi

Autentikasi adalah isu yang lain dalam internet banking. Transaksi pada internet atau jaringan telekomunikasi yang lain harus aman untuk memperoleh kepercayaan dari publik. Pada lingkungan *cyber*, seperti pada dunia nyata yang sebenarnya, *customer*, bank memerlukan jaminan bahwa mereka akan memperoleh *service* seperti yang mereka inginkan dan mereka tahu identitas orang yang berinteraksi dengannya.

Dalam hal ini, bank biasanya menggunakan teknologi kriptografi dengan algoritma simetri (*private key*) untuk menjamin keamanan dari pesan dan algoritma asimetri (*public/private key*) untuk melakukan autentikasi. Algoritma asimetri memiliki dua buah kunci yaitu *public key* dan *private key*. Kedua kunci ini berbeda, tetapi tidak bisa terlepas dari yang lain (saling berpadanan). Contoh: autentikasi sebuah pesan yang datang dari pengirim, pengirim harus mengenkripsi pesan dengan menggunakan kunci *private*, dimana hanya pengirim yang mengetahui kunci *private*. Dalam pembacaan pesan, pesan hanya dapat dibaca dengan menggunakan kunci publik dari pengirim. Oleh karena itu, penerima yang mengetahui pesan tersebut datang dari pengirim yang diharapkan, dapat membaca pesan dengan kunci publik dari pengirim.

Algoritma kriptografi asimetri (kunci publik) yang umum digunakan adalah RSA, yang menggunakan panjang kunci mencapai 1024 bit. Dengan menggunakan dua bentuk algoritma kriptografi, simetri untuk melindungi pesan dan asimetri untuk melakukan autentikasi, bank dapat menjamin keamanan pesan dan memiliki kepercayaan yang tinggi untuk menjaga identitas dari *customer*.

Perangkat biometrik (*biometric devices*) adalah bentuk autentikasi yang berkembang saat ini. Perangkat ini dapat mengambil bentuk berupa scan retina, jari, atau suara. Penggunaan perangkat biometrik saat ini belum umum, hanya dipakai oleh beberapa bank untuk melakukan autentikasi.

2.3 *Trust*

Isu yang lain dalam sistem internet banking adalah *Trust*. Seperti yang diberitahukan pada bab sebelumnya, kriptografi algoritma kunci publik dapat digunakan untuk keamanan informasi dan mengautentikasi transaksi yang terjadi. Dalam hal ini, kepercayaan dari pihak ketiga diperlukan pada proses transaksi. Oleh karena itu pada pihak ketiga dikenal dengan adanya *certificate authority*.

Sebuah *certificate authoriy* adalah sebuah pihak ketiga yang terpercaya yang memverifikasi identitas dalam lingkungn *cyber* (pemegang hak otorisasi). Konsep dasarnya adalah, bahwa sebuah bank atau pihak ketiga yang lain menggunakan sertifikat tersebut untuk memvalidasi pihak lain yang terlibat dalam transaksi.

2.4 *Nonrepudiation*

Dalam hal ini, pengirim tidak dapat menyangkal mengenai isi pesan yang dikirim olehnya. Dimana, antara pengirm dan penerima memiliki suatu bukti mengenai keabsahan pesan yang dikirim. Untuk menangani hal ini, internet banking menggunakan algoritma kriptografi kunci publik, contoh: autentikasi e-mail, mencegah penyangkalan oleh pengirim maupun penerima.

2.5 *Privacy*

Privacy adalah isu yang meningkat saat ini. Hal ini terjadi karena begitu banyaknya kejadian di lingkungan *cyber* yang berusaha untuk memperoleh/merusak *privacy* orang lain untuk sesuatu hal. Dengan semakin berkembangnya berkembangnya transaksi melalui internet banking, sebuah bank harus merespon dan menangani hal ini untuk memberikan pandangan yang positif bagi *customer* dan memberikan keuntungan baginya.

3. Penerapan Kriptografi

Sekarang ini, bisnis termasuk kegiatan perbankan telah mengalami perubahan dari aktivitas fisik ke aktifitas berbasis elektronik. Hal ini mencakup penjualan barang dan jasa, pertukaran data elektronik, transfer dana atau uang, dan internet banking itu sendiri. Dalam menghadapi perubahan ini, pengelola bank harus harus melakukan pengontrolan dengan cara yang berbeda. Hal dasar yang dibutuhkan dalam pengontrolan ini adalah kerahasiaan data, kepercayaan, verifikasi dan yang menjadi hal paling penting adalah pengamanan autentikasi internet banking.

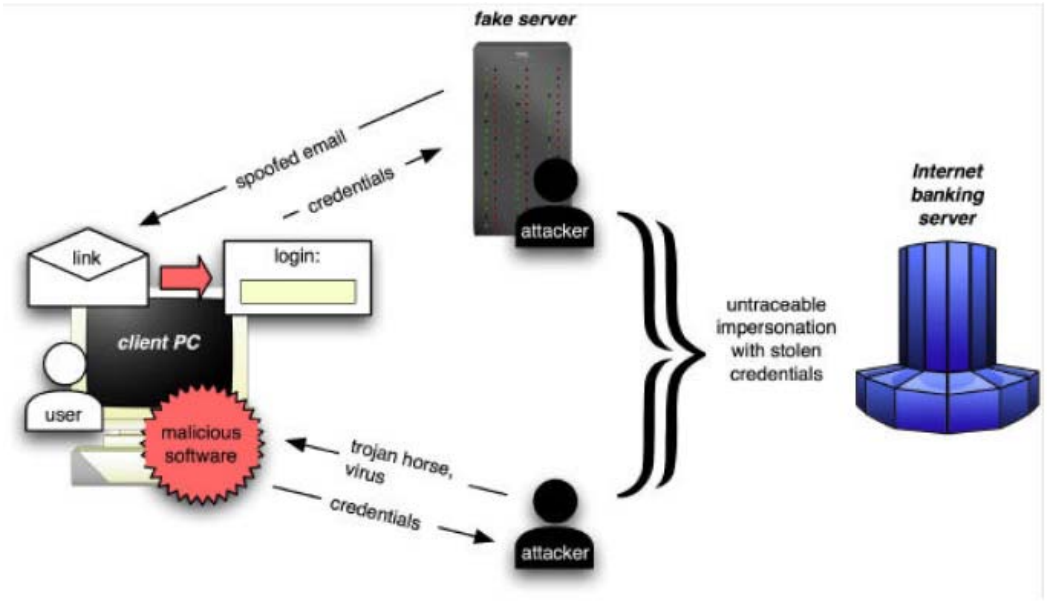
3.1 Klasifikasi pengamanan autentikasi internet banking

Suatu sistem internet banking harus melakukan autentikasi terlebih dahulu sebelum memberikan hak akses terhadap layanan-layanan yang diberikan. Dengan kata lain, sistem internet banking harus mengetahui apakah pihak yang melakukan transaksi adalah nasabah yang sah. Hal ini dilakukan dengan menanyakan hal-hal yang rahasia kepada nasabah yang melakukan transaksi.

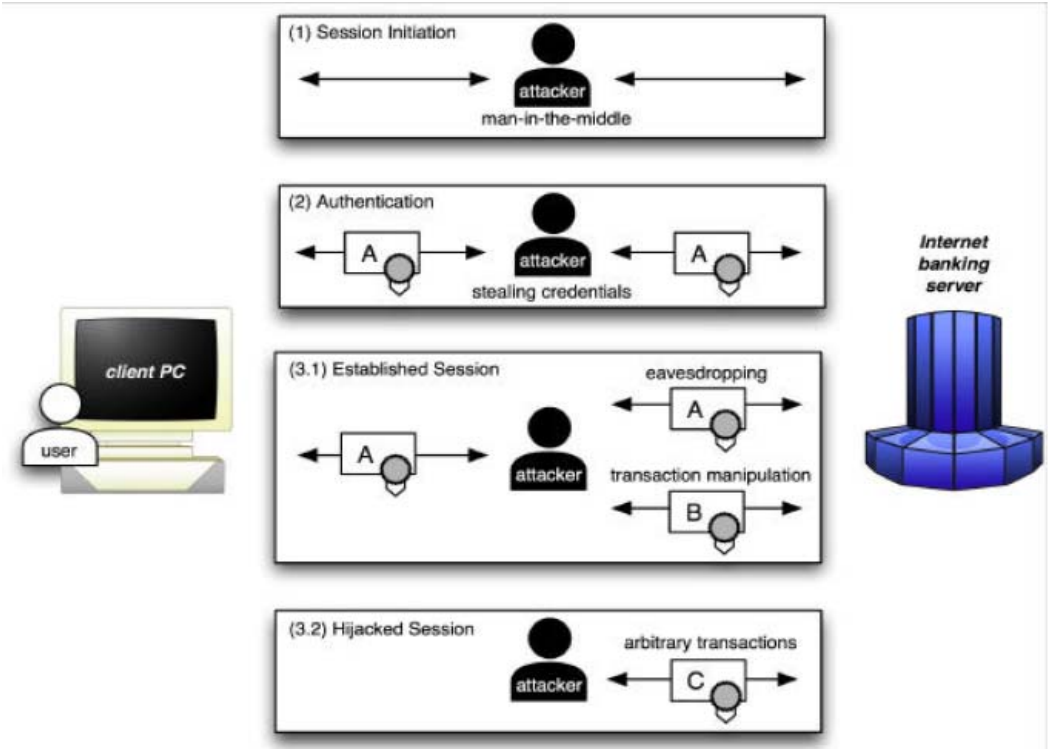
Secara umum, metode-metode autentikasi internet banking dapat diklasifikasikan berdasarkan kemampuan metode tersebut dalam melawan dua jenis serangan yang umum yaitu: serangan pencurian informasi-informasi rahasia secara *offline* dan serangan terhadap jalur komunikasi *online*.

Pencurian informasi rahasia secara *offline* bertujuan untuk mengumpulkan informasi-informasi penting mengenai seorang nasabah bank dengan menggunakan virus, trojan, atau *software* lainnya. Pengamanan yang dapat dilakukan untuk mengatasi masalah ini yaitu dengan menggunakan firewall untuk mengamankan jaringan, penggunaan antivirus, dan pengkonfigurasian komputer dengan benar.

Serangan terhadap jalur komunikasi *online* seperti “man-in-the-mindle”, merupakan serangan yang lebih berbahaya dan sangat penting untuk ditangani. Berbeda dengan pencurian informasi secara *offline*, dalam serangan komunikasi *online* pencurian pesan-pesan yang dikirimkan akan sulit untuk diketahui. Penyusup akan memalsukan identitas dirinya yang berperan sebagai server sistem *online* banking. Secara umum, walaupun kemunikasi yang berjalan menggunakan SSL/TSL, tetapi seringkali nasabah tidak memperhatika keaslian sertifikat yang dimiliki oleh server. Akibatnya komunikasi akan berjalan secara normal tetapi dengan server yang salah.



Gambar 1 Skenario pencurian informasi rahasia secara *offline*



Gambar 2 Skenario serangan terhadap jalur komunikasi *online*

Secara umum ada dua jenis autentikasi yang digunakan dalam mengatasi serangan *offline* dan *online* yaitu short -time password (one time password) dan *public key infrastructure* (PKI) atau komunikasi berbasis sertifikat.

3.2 Short time password

Short time password merupakan suatu cara yang dapat digunakan untuk mengatasi masalah pencurian informasi secara *offline*. Autentiksi short time password menggunakan kriptograpfi simetri yang dikombinasikan dengan modul *security* berupa *hardware* (smart card) dan smart card reader *offline* (*stand alone*).

Inti dari metode ini adalah sebuah smart card yang di personalisasi dengan key kriptografi simetri secara random (3DES/AES) yang diproteksi dengan menggunakan pin yang digunakan untuk menyimpan atau menghasilkan password yang digunakan untuk melakukan transaksi. Penggunaan kriptografi simetri bertujuan untuk mengahasilkan password dengan ukuran yang lebih pendeng sehingga memudahkan *user* untuk menggunakannya. Password yang dihasilkan dibaca dengan menggunakan *offline* card reader dengan memasukkan PIN yang digunakan untuk memproteksi smart card.

Berikut adalah skenario proses autentikasi dengan menggunakan short time password.

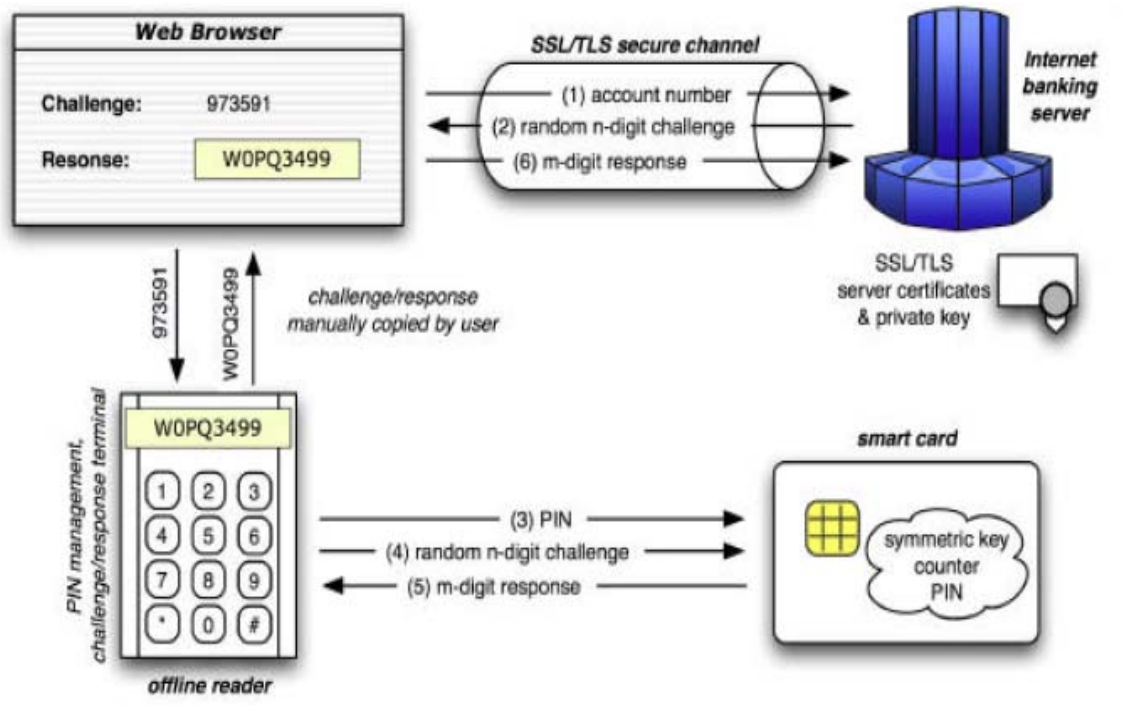
1. *User*/nasabah berkomunikasi dengan server bank dengan menggunakan jalur SSL/TSL dengan menggunakan server-side autentication. Dengan metode ini maka *user* dapat menjamin bahwa dia berkomunikasi dengan bank yang sah.

2. *User* memasukkan informasi berupa identitas (login id), selanjutnya bank memberikan n-digit rahasia dan meminta kembalian berupa n-digit rahasia dari *user*.

3. *User* membuka smar card dan memasukkan n-digit rahasia yang diterima dari bank. Selanjutnya smart card melakukan kalkulasi dengan mengenkripsi n-digit dari bank, menambahkan symetric key dan meng-encode hasilnya ke dalam bentuk string yang mudah untuk dibaca.

4. Selanjutnya *user* memasukkan hasil kalkulasi ke form login untuk memulai transaksi.

Skema ini sangat berguna dalam mengatasi pencurian informasi secara *offline* karena informasi *user* disimpan dalam sebuah smart card yag diproteksi dengan menggunakan PIN dan dibaca dengan *offline* smart card reader. Dengan cara ini maka penyerang tidak bisa menggunakan *software*, trojan atau virus untuk mencuri informasi pribadi dari *user*. Penyerang juga tidak bisa memalsukan halaman login karena tidak bisa menghasilkan n-digit kode rahasia yang digunakan dalam proses autentikasi *user*



Gambar 3. Skenario proses autentikasi dengan short time password

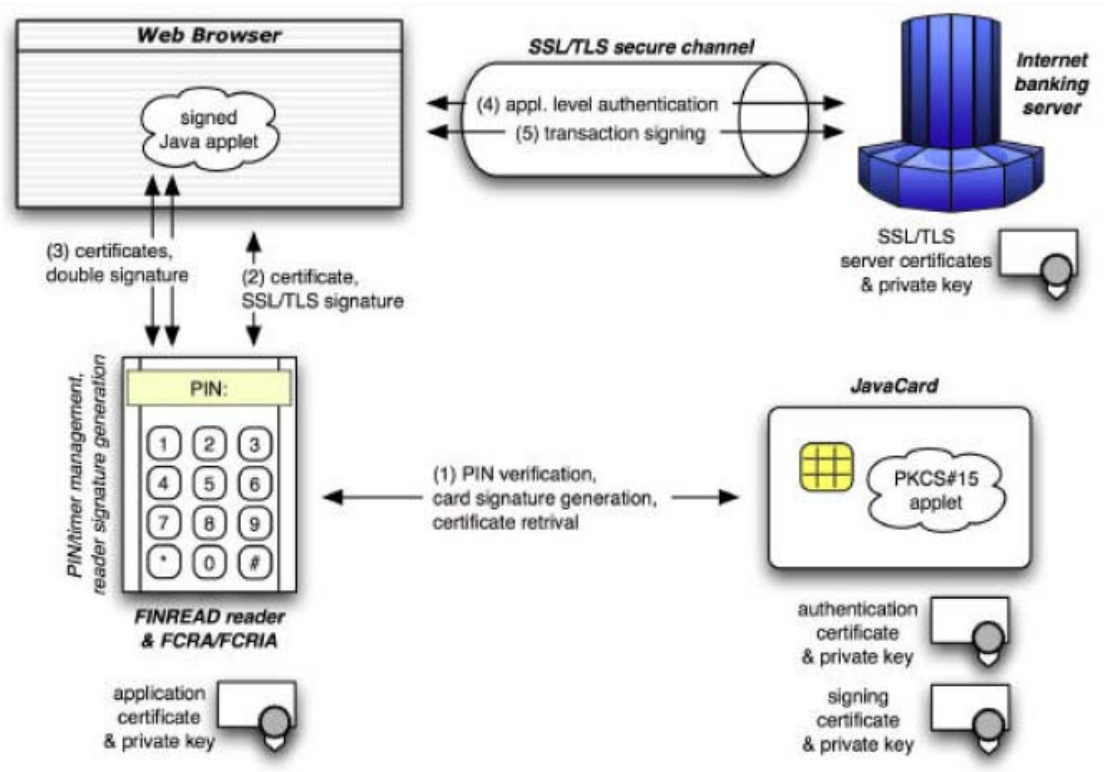
3.3 Public Key Infrastructure (Certificate-Based)

Public Key Infrastructure atau komunikasi berbasis sertifikat merupakan suatu cara yang dilakukan untuk menangani serangan komunikasi *online*. PKI menggunakan algoritma kriptografi asimetri seperti RSA (Rivest Shamir Adlemann) atau ECC (Eliptic Curve Cryptogaphy). Pada awalnya, setiap *user* memilkisi sepasang kunci privat dan public yang saling bersesuaian dan sebuah sertifikat yang dikeluarkan oleh pihak yang terautorisasi yang sesuai dengan kunci yang dimiliki oleh *user*. Sertifikat tersebut merupakan sebuah bukti bahwa sebuah public key bersesuaian dengan nama pemiliknya dan *user* tersebut memiliki kunci privat yang bersesuaian. Kunci privat dan sertifikat digunakan untuk membentuk komunikasi SSL/TSL yang aman.

Hal yang menjadi perhatian utama adalah perlindungan terhadap kunci privat yang dimiliki oleh *user*. Jika kunci tersebut disimpan didalam komputer *user*, maka akan terancam akan pencurian informasi *user* dengan menggunakan trojan atau virus. Untuk mengatasi hal ini maka kunci rahasia *user* disimpan dalam sebuah media seperti smart-card atau javaCard. Dengan cara ini maka pencurian terhadap kunci privat akan sulit bahkan tidak bisa dilakukan karena selain medianya adalah smart-card yang sulit untuk

diakses, media tersebut juga diproteksi dengan menggunakan PIN tertentu.

Skenario autentikasi dengan menggunakan kunci privat yang tersimpan dalam smart card/javaCard dapat dilihat dalam gambar berikut:



Gambar 4 Skenario autentikasi dengan menggunakan kunci privat yang disimpan dalam javaCard

4. Kesimpulan

Ada beberapa kesimpulan yang dapat diambil dari penerapan kriptografi dalam internet banking yaitu:

1. Aspek keamanan dalam komunikasi melalui jaringan komputer menjadi semakin penting terutama karena banyaknya aktivitas pertukaran informasi rahasia melalui Internet, contoh: internet banking.
2. Penerapan autentikasi dalam transaksi internet banking merupakan faktor yang sangat penting untuk mendukung transaksi berjalan dengan baik.
3. Autentikasi dengan short time password dan *public key infrastructure* (*certificate based)* merupakan konsep kriptografi yang dapat diterapkan pada internet banking.
4. Keamanan informasi-informasi penting dalam melakukan transaksi diinternet tidak bisa sepenuhnya dipercayakan kepada system yang sudah berjalan tetapi membutuhkan ketelitian pengguna dalam melakukan tansaksi.

8. Referensi

[1] *First Republic Banking Online Privacy*, http://www.firstrepublic.com, diakses tanggal 4 Januari 2006 pukul 15:37.

[2] *Consumer e-Banking andOn-Line Coorporate Banking Solutions* , http://www.intel.com, diakses tanggal 5 Januari 2006 pukul 14:05.

[3] R. F. Churchhouse, *Code and Ciphers: Julius Caesar, the enigma and the Internet*,Cambridge University Press, 2002

[4] *safeWord for onlineBanking*, http:// www.securecomputing.com, diakses tanggal 5 Januari 2006 pukul 16:07.