INFRASTRUKTUR KRIPTOGRAFI PADA SECURITY TOKEN UNTUK KEPERLUAN INTERNET BANKING

Petra Novandi Barus
Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung, Indonesia
petra.barus@gmail.com

ABSTRAKSI

Internet banking *atau perbankan internet adalah salah satu fasilitas layanan perbankan yang ditujukan bagi nasabah untuk dapat melakukan transaksi perbankan melalui situs internet yang telah disediakan oleh bank bersangkutan. Maraknya penggunaan internet dikalangan masyarakat membuat layanan ini makin dipakai oleh banyak nasabah untuk melakukan transaksi karena kemudahannya. Berbeda dengan ATM, nasabah dapat menggunakan fasilitas ini tanpa memakai komputer yang telah disediakan oleh bank. Keunggulannya ini lah yang membuat internet banking menjadi sangat rawan keamanannya.*

Karena nasabah menggunakan komputer bukan dari bank, maka ancaman keamanan yang dapat terjadi antara lain phising*,* keylogger*, dan* man in the middle*. Hal ini disebabkan karena bank tidak dapat mengatur keamanan dari komputer yang dipakai oleh nasabah. Komputer tersebut sewaktu-waktu bisa dimodifikasi oleh pihak lain sedemikian rupa sehingga pesan-pesan transaksi yang ada pada transaksi menjadi tidak rahasia dan tidak utuh. Untuk melindungi kepentingan nasabah maka bank yang memiliki layanan* internet banking *biasanya menambahkan lapisan keamanan yakni* security token.

Makalah ini membahas implementasi kriptografi yang digunakan dalam penggunaan security token *yakni kunci asimetrik,* one-time password*, dan komunikasi terenkripsi. Makalah ini juga membahas contoh penggunaan* security token *dalam penggunaan* internet banking *di Indonesia.*

Kata kunci : Kriptografi, *Security Token, Internet Banking*

1. PENDAHULUAN

Internet Banking

Internet Banking atau perbankan internet adalah sebuah layanan yang disediakan oleh bank yang dapat memfasilitasi nasabahnya untuk melakukan transaksi perbankan melalui situs internet. Dengan menggunakan layanan ini, nasabah tidak perlu mendatangi kantor bank dan juga ATM untuk melakukan transaksi. Nasabah hanya memerlukan koneksi internet dan mengunjungi situs yang telah disediakan untuk pelayanan. Setelah melakukan autentikasi pada situs tersebut, nasabah dapat melakukan transaksi yang diinginkan sesuai menu yang disediakan oleh situs. Sama halnya dengan layanan perbankan populer seperti SMS Banking, nasabah dapat melakukan transaksi di mana saja dan kapan pun juga asalkan tersedia jaringan internet.

Layanan ini sudah ada di dunia sejak awal dekade 1980an salah satunya oleh Nottingham Building Society pada tahun 1983 di Inggris. Sedangkan di Indonesia, fasilitas ini pertama kali digunakan oleh Bank Papan Sejahtera pada awal dekade 1990an meski kemudian pada tahun 1995 bank ini ditutup karena masalah keuangan. Akan tetapi kini telah banyak bank di Indonesia yang telah menyediakan layanan serupa : Bank Mandiri, Bank BCA, Bank Niaga, Citibank, dan lain-lain.

Keamanan pada *Internet Banking*

Hal-hal yang menjadi ancamanan pada internet banking antara lain *phising*, *keylogger*, dan *man in the middle*.

Phising adalah upaya untuk mencuri data pribadi seperti nama pengguna, sandi lewat, dan nomor rekening dengan cara meniru sebagai instansi terkait pada jalur komunikasi elektronik. Salah satu contoh *phising* adalah meniru sebuah situs milik bank tempat nasabah melakukan transaksi atau mengirim surat elektronik kepada nasabah dengan berpura-pura sebagai bank terkait untuk meminta data pribadi yang diperlukan. Kegiatan yang pertama lebih sering disebut dengan *website spoofing.*

Keylogger adalah sebuah aplikasi yang berjalan secara tersembunyi pada sistem operasi sebuah komputer yang digunakan terutama untuk merekam aktivitas pengguna komputer tersebut. Dalam hal ini, aplikasi ini memberi ancaman yakni merekam nama pengguna serta sandi yang dimasukkan oleh nasabah pada situs *internet banking*. Para pemasang *keylogger* kemudian dapat mengambil rekaman tersebut dan menggunakannya untuk hal-hal yang tidak diinginkan.

Gambar 1. ***Internet Banking Bank BCA***

Man In The Middle, adalah sebuah serangan di mana penyerang dapat membaca dan memodifikasi pesan-pesan yang dikirim oleh nasabah dengan sistem informasi bank atau sebaliknya.
Karena begitu banyaknya ancaman keamanan pada fasilitas *internet banking* maka sekarang bank-bank menambahkan lapisan keamanan yang lebih tinggi yakni berupa *security token.*

Security Token

Di dalam mengautentikasi seseorang ada 3 macam hal yang digunakan untuk diidentifikasi dari orang tersebut.

1. *Something that user knows*, yakni sesuatu yang diketahui oleh pengguna seperti tanggal lahir, nama ibu, sandi lewat, PIN dan lain-lain.
2. *Something that user has*, yakni sesuatu yang dimiliki oleh pengguna seperti sidik jari, retina mata, dan lain-lain.
3. *Something that user is,* yakni siapa pengguna tersebut.

Security Token adalah sebuah objek fisik yang digunakan untuk autentikasi pada sebuah sistem. Alat ini biasanya didesain berukuran kecil sehingga dapat dibawa-bawa oleh nasabah dan kemudian dapat digunakan sewaktu-waktu untuk melakukan transaksi.
Di dalam proses pengautentikasian, *security token* termasuk di dalam *something that user has*. Selain mengautentikasi nama dan sandi, bank juga perlu mengetahui tanda dari *security token* yang dimiliki oleh nasabah yakni data-data yang dimiliki oleh *security token tersebut.*
Bentuk-bentuk *security token* sangatlah bervariasi. Akan tetapi seperti yang disebutkan di *atas, security token* biasanya berukuran kecil sehingga dapat dibawa-bawa oleh nasabah. Contoh bentuk-bentuk security token antara lain

1. Smart card
2. ID card
3. Papan bertombol
4. Handphone
5. Gantungan kunci
6. Pemancar *Infrared/Bluetooth*

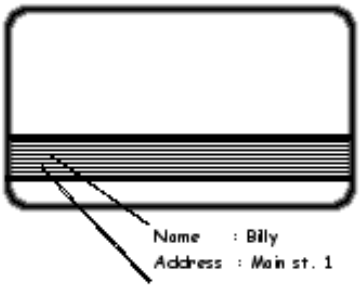
Dengan adanya *security token* diharapkan keamanan pada sistem perbankan internet menjadi lebih kuat sehingga dapat melindungi kepentingan nasabah dan menumbuhkan kepercayaan nasabah pada bank.

2. IMPLEMENTASI KRIPTOGRAFI PADA SECURITY TOKEN

Hal-hal yang menjadi fungsi jenis security token yang umum ada dan telah banyak dipatenkan : infrastruktur kunci publik, *one time password,* jalur komunikasi *(communcation* means)..

1. Infrastruktur Kunci Publik

Security token jenis ini berisi data identitas pengguna yang digunakan untuk penandatanganan dijital. Dengan menggunakan infrastruktur kunci asimetrik, maka autentikasi yang dilakukan menjadi lebih aman.



Gambar 2. ***Smart Card***

Autentikasi pengguna ini berhasil dilakukan setelah pengguna menandatangani sejumlah data yang ditunjuk oleh protokol keamanannya (seperti SSL). Tandatangan dijital tersebut dihasilkan dari perhitungan yang dilakukan *security token* yang dilaksanakan setelah pengguna melakukan autentikasi pemegangan *security token*, seperti sandi lewat atau PIN (*personal identification number*)
Setelah autentikasi berhasil biasanya data mengenai pengguna seperti nama, alamat, tanggal kadaluarsa, diekstraksi oleh *server* masih menggunakan infrastruktur kunci publik untuk keperluan transaksi yang dilakukan oleh pengguna.

2. One Time Password

Security token jenis ini digunakan untuk menghasilkan sandi lewat yang hanya dapat digunakan sekali karena sandi ini akan terus berubah. Jenis ini digunakan untuk mengelabui lawan yang mengintip sandi yang dimasukkan oleh pengguna. Lawan tersebut tidak akan bisa memasukkan sandi yang sama kemudian karena sandi sudah berubah.
Salah satu cara untuk membangkitkan sandi ini dengan menggunakan fungsi *hash*. Pengguna diminta untuk memasukkan sebuah *string* S_0 dan sebuah bilangan N kemudian memilih

sebuah fungsi *hash* $f(x)$ yang digunakan untuk membangkitkan sandi tersebut. Pada kali pertama, sandi yang dibangkitkan adalah *string* S_0 yang di*hash* sebanyak N kali. Kemudian untuk kali kedua, sandi akan dibangkitkan dengan sandi sebelumnya yang di*hash* sebanyak $N-1$ kali. Setelah kali ke N maka jumlah *hash* yang akan dilakukan dikembalikan ke N kali. Bilangan N ini akan dicatat baik di sisi *client* maupun di sisi *server.*

$$S_1 = f(f(...(f(S_0)))..)$$

$$S_2 = f(f(...(f(S_1)))..)$$

$$S_3 = f(f(...(f(S_2)))..)$$

....

$$S_N = f(S_{(N-1)})$$

$$S_{(N+1)} = f(f(... \ (f(S_N)))..\ )$$

Gambar 3. *One Time Password*

Salah satu cara lain untuk membangkitan kunci adalah dengan menggunakan interval waku yang tersinkronisasi.
Ketika sebuah token dirilis, maka di dalam token tersebut diinisialisasi sebuah nilai yang kemudian dicatat oleh *server.* Nantinya setiap interval tertentu nilai tersebut akan berubah pada keduanya. Hanya saja perubahannya terjadi sedemikian sehingga nilai tersebut selalu tetap sama antara *server* dan *client.*

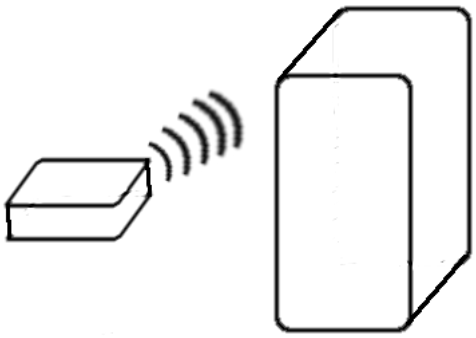
Waktu	**Server**	**Client**
00:00	abcdefghijk	abcdefghijk
00:08	asdasdagab	asdasdagab
00:16	oeqgqwgdb	oeqgqwgdb
00:24	isdfagai	isdfagai

Tabel 1. Pembangkitan Sandi

Pembangkitan sandi dapat dilakukan dengan menggunakan algoritma *pseudorandom* atau juga dengan menggunakan fungsi *hash* seperti yang dilakukan pada metode *one-time password* yang sebelumnya dengan nilai inisialisasi tersebut sebagai *seed*nya.

3. Communication Means

Security token jenis ini adalah *security token* yang dapat mentransmisikan datanya kepada *server. Security token* ini biasa diimplementasikan dalam bentuk *RFID* atau *Bluetooth.*



Gambar 4. *Bluetooth Security Token*

Ketika *server* mendeteksi keberadaan *token,* maka dengan segera *server* membangun sebuah jalur komunikasi aman dengan menggunakan pengenkripsian. Tujuannya adalah supaya data yang ditransmisikan tidak dicuri dengar oleh pihak lawan. Setelah jalur tersebut dibangun maka *server* akan mengautentikasi *token* berdasarkan data yang dimiliki oleh *token* tersebut.
Selain itu *token* juga bisa digunakan dengan menggunakan jalur komunikasi lain seperti kabel data atau juga port USB (*Universal Serial Bus*)

Selain di atas, masih banyak lagi jenis-jenis *security token* lainnya yang sedang dikembangkan.

3. SECURITY TOKEN UNTUK KEPERLUAN INTERNET BANKING

Seluruh *token* yang digunakan dalam fasilitas internet banking adalah *token* yang termasuk ke dalam jenis *token* yang dapat membangkitan *one-time password.* Sebagai contoh, penulis mengambil penyedia layanan *internet banking* yakni Bank BCA dan Bank Mandiri. Untuk layanan yang diberikan Bank BCA, *token*nya diberi nama KeyBCA sedangkan Bank Mandiri diberi nama PIN Mandiri.

Gambar 5. KeyBCA

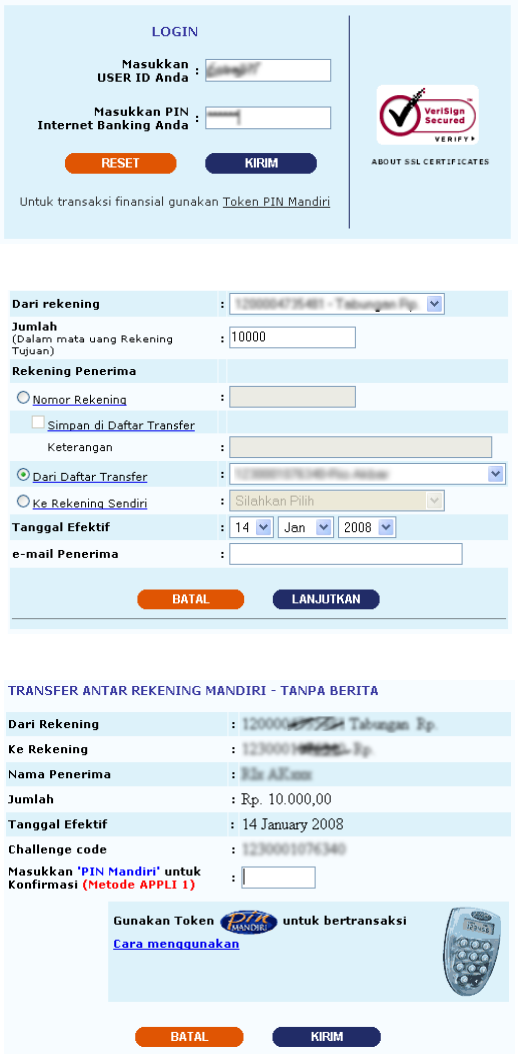
Gambar 6. PIN Mandiri (*milik penulis*)

Gambar 7. Vasco Digipass 260

Kedua jenis token yang digunakan oleh kedua bank adalah token yang dikeluarkan oleh Vasco, sebuah perusahaan yang bergerak dibidang keamanan data di internet, yakni jenis DP250, DP250i, serta DP300 dengan menggunakan *server Velis Authenticator* (*Server VA*). Cara kerja *token* ini adalah dengan membangkitkan *one-time password* berdasarkan waktu.
Jenis aplikasi yang terdapat pada token jenis ini adalah

1. Aplikasi *Response Only* (RO), aplikasi ini memiliki 2 variable yaitu, *seed valu*e dan *current time* untuk membangkitkan sandi atau PIN.
2. Aplikasi *Challenge Response* (C/R), aplikasi ini memiliki 3 *variable* yaitu, *seed value* yakni nilai yang diinisialisasi pada awal perilisan token, dan *current time* (waktu pada saat *token* digunakan) dan *challenge* yaitu berupa angka dengan digit tertentu yang digenerate oleh server VA yang harus di input ke dalam token, untuk membangkitkan sandi atau PIN.

   Biasanya untuk Bank Mandiri, *challenge code* yang digunakan adalah rekening penerima transfer (jika menggunakan transfer) atau nomor tertentu milik *recipient.*
3. Aplikasi *Digital Signature,* aplikasi ini mirip dengan C/R, hanya saja *challenge* yang disediakan lebih dari 1 *challenge* (max 8) yang dapat diinputkan kedalam *token*, dan *challenge* ini tidak berasal dari server VA, bisa berupa angka dari mana saja. fungsi dari aplikasi ini salah satunya adalah untuk transfer uang antar rekening. field/challenge yang digunakan olek BCA/Mandiri adalah 3 buah. Field : nomor rekening pengirim, nomor rekening tujuan, dan nominal tranfer. Ketiga nilai ini akan dikomputasikan oleh token menjadi sebuah nilai lagi yang nantinya akan menjadi *seed* untuk sandi.



Gambar 8, 9, 10. Proses Transaksi

Seperti yang terlihat pada gambar 10, situs *Internet Banking*, membangkitkan nilai yakni *challenge code* yang akan dimasukkan ke dalam *token*. Dari c*hallenge code* ini kemudian dibangkitkan kunci konfirmasi yang digunakan oleh *server* untuk mengautentikasi.

Karena *token* ini bekerja berdasarkan waktu, maka sewaktu-waktu jika *token* kehabisan baterai atau karena suatu hal jam internal yang ada di dalam *token* tidak sinkron maka nasabah pemegang *token* diharuskan untuk segera menghubungi *costumer service.*

4. KESIMPULAN

Dengan menggunakan fasilitas *Internet Banking*, nasabah dapat dengan mudah melakukan transaksi perbankan dengan menggunakan internet. Fasilitas ini sudah banyak disediakan oleh bank-bank di Indonesia seperti Bank Mandiri dan BCA. Akan tetapi fasilitas ini rawan serangan keamanan seperti *phising, keylogger*, dan *man in the middle*. Oleh karena itu dengan menggunakan implementasi kriptografi berupa *security token*, maka kerahasiaan dan kepentingan nasabah dapat dilindungi dengan baik untuk meningkatkan kepercayaan nasabah terhadap bank.

REFERENSI

[1] Agam, Leedor *et.al. Security Token*. World Intellectual Property Organization. 2004. Patent no. PCT/II.2004/000628

[2] De Cock, Deni *et.al. Threat Modelling For Security Tokens In Web Applications*. COSIC Research Group, Katholieke Universiteit Leuven. Belgium, 2004.

[3] Internet Banking Mandiri. http://ib.bankmandiri.co.id Terakhir di akses 14 Januari 2007.

[4] Munir, Rinaldi. *Bahan Kuliah IF5054 Kriptografi*. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung. 2006. Bandung.

[5] Rollier, Alain et. al. *Security Token And Method For Authenticating Of A User With The Security Token*. World Intellectual Property Organization. 2006. Patent no. PCT/CH2006/000715

[6] Vasco. Strong User Authentication. http://www.vasco.com Terakhir akses 9 Januari 2007.