MANAJEMEN KUNCI KRIPTOGRAFI DENGAN SECURITY TOKEN DAN IMPLEMENTASINYA PADA TOKEN PIN BANK MANDIRI

Bemby Bantara Narendra – NIM : 13503105

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13105@students.if.itb.ac.id

Abstrak

Beberapa tahun terakhir bank-bank besar berlomba-lomba mengeluarkan layanan internet banking. Namun layanan ini tidak sepenuhnya aman. Seperti beberapa waktu sebelumnya, banyak nasabah pengguna layanan serupa yang dikeluarkan BCA mengalami kebobolan rekening. Pelaku kriminal Internet berhasil memperdaya nasabah antara lain dengan *phishing* atau dengan membuat situs yang menyerupai situs internet banking yang dikeluarkan BCA dan merekam identitas nasabah yang terjebak ke dalamnya.

Untuk menghindari kejahatan internet, internet banking yang dikeluarkan Bank Mandiri menggunakan perangkat keras yang disebut token PIN Mandiri. Bentuknya menyerupai kalkulator dengan ukuran sekitar 3 x 5 sentimeter. Token tersebut merupakan alat untuk membuat one time password atau password dinamis yang hanya dapat satu kali digunakan. Token menjadi alat untuk authentikasi terhadap user ketika ingin masuk ke dalam sistem bank. Jika selama ini password yang biasa kita gunakan adalah static, token berfungsi untuk men-generate password tersebut setiap satuan waktu tertentu.

Kekuatan sistem kriptografi secara total bergantung pada keamanan kunci. Kunci perlu dilindungi selama fase daur hidupnya. Daur hidup kunci dimulai dari pembangkitan kunci (generation) sampai kunci tidak diperlukan lagi untuk kemudian dihancurkan (destruction).

Makalah ini akan membahas mengenai manajemen kunci kriptografi dengan menggunakan security token dan studi kasus implementasinya pada bank Mandiri yang telah menggunakan token PIN Mandiri dalam melindungi transaksi internet bankingnya.

Kata Kunci : token mandiri, security token, two-factor authentication, vasco, keybca

1. Pendahuluan

Internet banking merupakan inovasi dari penerapan teknologi informasi dalam dunia perbankan. Dengan menggunakan internet banking, customer sebuah bank dapat melakukan berbagai macam transaksi perbankan dari rumah dengan berbekal komputer dan koneksi internet. Namun masih banyak yang meragukan keamanan transaksi perbankan lewat internet banking ini karena adanya kemungkinan-kemungkinan data rahasia customer yang dapat dibobol.

Saat ini customer tidak perlu mengalami kekhawatiran terhadap keamanan transaksi

internet banking karena sebagian besar bank yang menggunakan teknologi internet banking telah dilengkapi dengan sistem keamanan berlapis untuk menjamin kerahasiaan data transaksi customernya. Semua transaksi yang dilakukan lewat Internet Banking juga lebih terlindungi berkat security token.

Security token adalah alat pengaman tambahan untuk melakukan transaksi finansial di internet banking. Security token ini berfungsi untuk mengeluarkan dynamic password atau PIN dinamis, yaitu PIN yang selalu berubah dan hanya dapat digunakan satu kali untuk tiap transaksi finansial yang dilakukan.

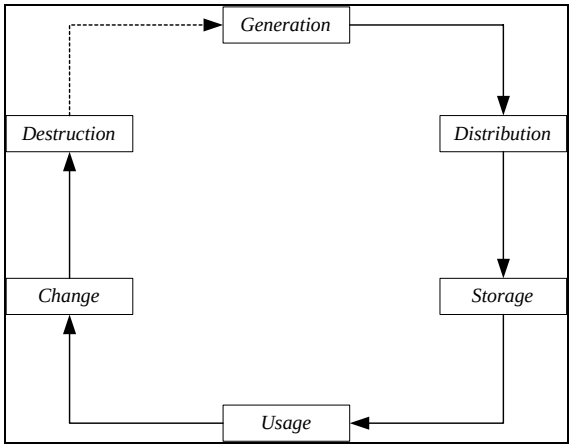
Keuntungan pemakaian security token ini adalah karena PIN selalu berganti setiap bertransaksi sehingga sukar dilacak oleh orang lain. Ditambah lagi token PIN ini unik bagi setiap nomor rekening dan tidak bisa digunakan pada rekening lain.

Dengan fasilitas ini, rekening customer tidak mungkin disalahgunakan meskipun informasi yang dimasukkan oleh customer telah tertangkap oleh orang lain (misalnya dengan menggunakan keylogger).

Pada bab berikutnya akan dibahas mengenai manajemen kunci kriptografi yang merupakan dasar dari pembuatan security token ini.

2. Manajemen Kunci Kriptografi

Kekuatan sistem kriptografi secara total bergantung pada keamanan kunci. Kunci perlu dilindungi selama fase daur hidupnya. Daur hidup kunci dimulai dari pembangkitan kunci (generation) sampai kunci tidak diperlukan lagi untuk kemudian dihancurkan (destruction). Secara garis besar, daur hidup kunci digambarkan pada Gambar 1 sebagai berikut ini:



Gambar 1. Daur hidup kunci

Tujuan manajemen kunci adalah menjaga keamanan dan integritas kunci pada semua fase di dalam daur hidupnya. Pada umumnya setiap kunci akhirnya diganti dengan kunci lain. Jadi, keseluruhan fase membentuk siklus (lingkaran) karena penghancuran kunci biasanya diikuti dengan penggantiannya dengan kunci baru (garis putus-putus).

Manajemen kunci yang dibahas difokuskan pada algoritma kriptografi simetri karena manajemen kunci untuk algoritma kunci-publik sangat berbeda dengan algoritma simetri.

Pembangkitan Kunci (Key Generation)

Pembangkitan kunci pada algoritma simetri jauh lebih mudah daripada pembangkitan kunci pada algoritma kunci-publik. Karena kunci simetri umumnya rangkaian bii atau rangkaian karakter, maka setiap pengguna dapat membangkitkan kuncinya sendiri.

Masalah utama yang muncul pada pembangkitan kunci adalah bagaimana membuat kunci yang tidak dapat diprediksi. Metode yang dapat digunakan untuk menjawab hal ini adalah dengan teknik manual (misalnya pelemparan koin/ dadu), pembangkitan dari data pribadi (misalnya PIN), atau menggunakan pembangkit bilangan acak.

Pada algoritma kunci-publik, pembangkitan kunci merupakan masalah tersendiri, karena

pembangkitan kunci membutuhkan perhitungan matematis yang rumit. Selain itu, pembangkitan bilangan prima yang besar juga dibutuhkan untuk membentuk kunci. Oleh karena itu, pada algoritma kunci-publik dibutuhkan program khusus untuk membangkitkan kunci.

Masalah yang timbul di sini adalah kepercayaan pengguna terhadap program tersebut. Pada RSA misalnya, bila program hanya dapat membangkitkan bilangan prima yang terbatas, maka pihak lawan dapat membangkitkan sendiri bilangan-bilangan prima yang terbatas itu dan menggunakannya sebagai faktor dari salah satu parameter RSA.

Penyebaran Kunci (Key Distribution)

Jika pengguna menggunakan kunci untuk melindungi informasi yang disimpan di dalam storage, maka tidak ada kebutuhan untuk menyebarkan kunci. Tetapi, untuk kebutuhan komunikasi secara aman, maka diperlukan kebutuhan untuk mengirimkan kunci. Protokol pertukaran kunci dengan menggunakan algoritma kunci-publik dapat digunakan untuk mendistribusikan kunci.

Penyimpanan Kunci (Key Storage)

Kunci disimpan di tempat yang aman yang tidak memungkinkan pihak lawan mengaksesnya. Oleh karena itu, penyimpanan kunci mungkin memerlukan perlindungan secara fisik (misalnya disimpan di dalam lemari besi). Alternatif lain, kunci dapat disimpan di dalam smart card yang hanya dapat dibaca dengan menggunakan kode rahasia.

Kunci sebaiknya disimpan tidak dalam bentuk jelas. Ada dua solusi alternatif untuk masalah ini.

1. kunci disimpan dengan mengenkripsinya dengan menggunakan kunci lain. Konsep ini mengarah pada konsep key hierarchy, yang dalam hal ini setiap kunci di dalam hirarkhi digunakan untuk melindungi kunci di bawahnya.
2. kunci dipecah menjadi beberapa komponen, setiap komponen disimpan di tempat terpisah. Jika kunci akan digunakan, maka setiap komponen direkonstruksi kembali.

Misalkan kunci K dibagi menjadi dua komponen, K1 dan K2. Membagi dua langsung K sedemikian sehingga setengah bagian pertama menjadi K1 dan setengah bagian sisanya menjadi K2 tidak dianjurkan, karena dapat memungkinkan pihak lawan menemukan K jika ia hanya mengetahui salah satu dari K1 dan K2.

Misalkan K panjangnya 64 bit, dan lawan mengetahui K1, maka K dapat ditentukan dengan hanya 232 percobaaan untuk menemukan K2 secara exhaustive search (lebih sedikit dibandingkan 264 percobaan).

Solusi pemecahan yang lebih baik adalah membentuk kunci K dari K1 dan K2 sedemikian sehingga $K = K1 \oplus K2$. Dalam hal ini, ukuran K1 dan K2 sama dengan ukuran K, sehingga jika salah satu dari komponen K1 atau K2 diketahui, maka K relatif lebih sukar ditentukan.

Penggunaan Kunci (Key Usage)

Setiap kunci digunakan sesuai tujuannya. Misalnya ada kunci yang digunakan untuk mengenkripsi pesan, dan ada kunci yang digunakan untuk mengenkripsi kunci lainnya. Supaya setiap kunci mempunyai penggunaan yang unik, maka kita perlu membeli label pada setiap kunci, yang dalam hal ini label menspesifikasikan penggunaan kunci.

Misalnya, label tersebut menspesifikasikan ‘kunci untuk mengenkripsi data’, ‘kunci untuk mengenkripsi kunci’, ‘kunci untuk pembangkitan bilangan acak’, dan sebagainya.

Untuk algoritma kunci-publik, pengguna perlu memberi label untuk dua pasang kunci yang setiap pasang terdiri dari kunci publik dan kunci rahasia. Satu pasang kunci untuk enkripsi dan satu pasang lagi untuk sidik dijital.

Perubahan Kunci (Key Change)

Kunci sebaiknya diubah secara periodik dan teratur. Sistem kriptografi harus mempunyai kemampuan untuk mengubah kunci. Kunci diubah secara teratur untuk membatasi lama keberadaanya dan mengurangi nilainya di mata penyerang. Pada sistem EFTPOS (Electronic Funds Transfer at Point of Sale), kunci diubah setiap kali setelah selesai satu transaksi.

Tidak ada aturan seberapa sering kunci seharusnya diubah. Tetapi cukup jelas dimengerti bahwa setiap kunci seharusnya diubah jauh sebelum ia dapat ditemukan dengan cara exhaustive search.

Penghancuran Kunci (Key Destruction)

Kunci yang tidak dibutuhkan lagi seharusnya dihancurkan dengan cara yang aman. Jika kunci dicatat pada media kertas, maka cara penghancurannya misalnya menggunakan alat pemotong kertas (crosscut), membakarnya, atau menguburnya.

Jika kunci disimpan di dalam media elektronik (seperti CD), maka cara penghancurannya bisa dengan menghapusnya atau menimpanya (overwritten) sedemikian sehingga tidak meninggalkan jejak yang bisa dilacak oleh penyerang. Kunci yang yang disimpan pada material lain dihancurkan sedemikian rupa sehingga ia tidak mungkin ditemukan kembali secara fisik maupun secara elektronik.

Bab berikutnya akan membahas lebih detail mengenai teknologi yang digunakan dalam security token cara kerja dari security token.

3. Security Token

Security token (atau kadangkala disebut juga dengan token hardware, authentication token, atau cryptographic token) merupakan alat fisik yang mengijinkan user berwenang dari suatu servis tertentu untuk dapat menggunakan servis tadi sebagai satu bentuk autentikasi.

Security token umumnya cukup kecil untuk dibawa dalam kantong atau dompet. Beberapa dapat menyimpan kunci kriptografis seperti digital signature, atau data biometrik seperti sidik jari. Beberapa didesain agar tahan terhadap goncangan dan ada juga yang didesain dengan beberapa tombol keypad yang memungkinkan pemasukan nomer PIN.

Tipe-tipe security token

Gambar 2. Beberapa tipe security token

Terdapat banyak vendor yang mengeluarkan security token dan menggunakan pendekatan masing-masing untuk membuat security token. Beberapa bahkan dipatenkan.

1. Digital signature

   Token yang mengijinkan pembangkitan kunci dilakukan pada token itu dan penyimpanan kunci privatnya dapat digunakan sebagai autentikasi user, karena privat key juga bisa digunakan sebagai bukti identitas user.

   Agar token dapat mengenali user, maka token harus memiliki suatu nomer yang unik. Token yang tidak dilengkapi dengan keypad atau keyboard atau antarmuka lainnya tidak dapat digunakan dalam beberapa skenario digital signature, seperti konfirmasi transaksi bank berdasarkan nomer akun bank yang dananya akan dikirimkan.

2. Single sign-on software

   Beberapa tipe dari solusi single sign-on menggunakan token untuk menyimpan software yang memungkinkan autentikasi dan pengisian password. Begitu password disimpan pada token maka user tidak perlu mengingat password-password mereka dan karenanya dapat memilih password yang lebih aman.

3. One-time passwords

   One-time password merupakan password yang selalu berubah setelah setiap kali login, atau berubah setiap interval waktu tertentu.

   a. One-time password berbasiskan algoritma matematika

      tipe lainnya dari one time password yang menggunakan algoritma matematika kompeks seperti fungsi hash kriptografi untuk menggenerate password baru berdasarkan password sebelumnya dan dimulai dari kunci shared rahasia.

      Contoh algoritma matematika lainnya yang digunakan dalam one-time password ini adalah adalah algoritma open source OATH yang telah distandardkan dan algoritma-algoritma lainnya yang telah dipatenkan.

      CRYPTOCard

      CRYPTOCard menghasilkan one-time password baru setiap kali tombolnya ditekan. Sistem komputer akan menerima beberapa nilai balasan jika tombolnya ditekan lebih dari sekali secara tidak sengaja atau jika clientnya gagal mengautentikasi.

      Verisign

      Verisign Unified Authentication menggunakan standard dari OATH.

Gambar 3. e-token milik Aladdin Knowledge System

      e-token Aladdin Knowledge System NG-OTP

      e-token Aladdin Knowledge System NG-OTP merupakan hibrid antara USB dan token one-time password. e-token Aladdin Knowledge System NG-OTP mengkombinasikan fungsionalitas dari token autentikasi yang berbasiskan smart card dan teknologi autentikasi user one-time password dalam mode terpisah.

   b. One-time password berbasiskan sinkronisasi waktu

      one-time password berbasiskan sinkronisasi waktu berubah secara konstan setiap satuan interval waktu tertentu, contohnya setiap satu menit. Untuk dapat melakukan hal ini, perlu dilakukan sinkronisasi antara token milik client dengan server autentikasi. Untuk token yang terpisah (atau disebut dengan disconected token), sinkronisasi waktunya dilakukan sebelum token diberikan kepada client. Tipe token lainnya melakukan sinkronisasi saat token

dimasukkan dalam suatu alat input.

Di dalam token terdapat sebuah jam akurat yang telah disinkronisasikan dengan jam yang terdapat pada server autentikasi. Pada sistem one-time password ini, waktu merupakan bagian yang penting dari algoritma password sehingga pembangkitan password baru didasarkan pada waktu saat itu dan bukan pada password sebelumnya atau sebuah kunci rahasia.

Booleansoft

Sinkronisasi token-token milik Booleansoft dengan server autentikasi dilakukan ketika dimasukkan ke dalam alat input seperti alat input USB atau drive CD-ROM. Token-token ini merupakan teknologi yang sudah dipatenkan juga.

Gambar 4. Token SecurID milik RSA Security

SecurID RSA Security

SecurID RSA Security menampilkan sebuah nomer yang berubah setiap interval. Client memasukkan one-time password bersama dengan sebuah PIN ketika mengautentikasi. Teknologi ini juga telah dipatenkan.

Gambar 5. Token DigiPass 260 milik VASCO

DigiPass Vasco

VASCO seri DigiPass memiliki keypad atau keyboard kecil dimana user dapat memasukkan pin dan kemudian menggenerate one-time password baru setiap 36 detik. Teknologi ini juga sudah dipatenkan.

DigiPass milik VASCO ini merupakan teknologi yang digunakan oleh token PIN Mandiri milik bank Mandiri dan token keyBCA milik bank BCA.

Token Autentikasi Seluler (CAT) Mega AS Consulting Ltd

Token Autentikasi Seluler (atau CAT) milik Mega AS Consulting Ltd adalah software token yang diproteksi PIN dan berjalan pada mobile device seperti telepon selular, PDA, dan Pocket PC.

Perbandingan terhadap kedua jenis one-time password

Terdapat beberapa manfaat penghematan yang jelas pada one-time password berbasis sinkronisasi waktu karena user cenderung menggenerate sebuah password dan tidak ada kemungkinan menuliskan

(password sebelumnya atau kunci shared) dengan salah. Melakukan kesalahan ini pada one-time password berbasis algoritma matematika akan menyebebkan client tidak tersinkronisasi dengan server autentikasi.

Sebagai alternatif, server perlu mempertimbangkan masalah ini (dengan mengacuhkan password yang salah dan dengan menerima misalnya maksimal sepuluh kali masukan password daripada sekedar hanya satu, dan juga bisa dengan menambah kemungkinan mekanisme re-sinkronisasi), sehingga akan ada ekstra usaha dalam implementasi yang dapat mempengaruhi harga sistem server.

Di sisi lain, terdapat beberapa manfaat pada one-time password berbasis algoritma matematika karena perangkat keras token tidak membutuhkan sebuah jam, sehingga token tidak perlu secara kontinyu diberi daya dan baterainya dapat bertahan lebih lama. Jika dihitung untuk instalasi dalam jumlah besar, one-time password berbasis sinkronisasi waktu dapat dianggap pilihan yang lebih mahal.

one-time password berbasis algoritma matematika juga rawan terhadap phishing. Pada akhir tahun 2005 kemarin, customer dari bank di Swedia tertipu dan memberikan one-time passwordnya. Namun, bahkan one-time password berbasis sinkronisasi waktu juga bisa menjadi rawan terhadap phishing, jika password digunakan cukup cepat oleh penyerang. Hal ini bisa dilihat pada tahun 2006 yang dialami oleh customer dari bank di Amerika Serikat.

Pada dasarnya, user dari sistem ini harus tetap waspada bahwa dia rawan terhadap serangan man-in-the-middle dan selayaknya tidak pernah memberikan one-time passwordnya pada pihak ketiga manapun.

Standardisasi merupakan langkah yang baik. Namun sayangnya sebagian besar teknologi one-time password berbasis sinkronisasi waktu yang baik telah dipatenkan dan tidak tersedia untuk dibagikan dengan masyarakat umum.

Model-model security token

Beberapa tipe token didesain terpisah (disconnected) sehingga mereka tidak memerlukan ala input. Beberapa tipe token lainnya memerlukan alat input. Pembeli dari solusi security token dapat dikenakan biaya tambahan dalam token yang menggunakan alat input yang mahal.

1. Bluetooth

   Token-token bluetooth sering dikombinasikan dengan token USB sehingga bekerja dalam kondisi terhubung maupun terpisah. Autentikasi bluetooth bekerja jika jaraknya kurang dari 10 meter. Jika bluetooth tidak tersedia, token harus ditancapkan dalam alat input USB agar dapat berfungsi.

2. Token disconnected

   Token disconnected merupakan bentuk yang paling umum digunakan pada saat ini. Contohnya adalah DigiPass milik VASCo dan SecurID milik RSA Security. Keuntungan penggunaan bentuk ini adalah tidak membutuhkan alat input apapun. Kekurangannya, token-token ini memiliki waktu hidup baterai yang relatif pendek, umumnya hanya tiga sampai dengan lima tahun saja, yang umumnya lebih kecil dibandingkan umur token USB yang dapat bertahan sampai dengan sepuluh tahun.

   Beberapa token seperti milik ActivIdentity memungkinkan penggantian baterai yang digunakan setelah baterai yang lama habis sehingga mengurangi biaya dari membeli token baru.

Gambar 6. Beberapa token milik ActivIdentity

3. PC card

   Token PC card dibuat hanya untuk bekerja pada laptop. PC card tipe II lebih banyak digunakan karena ukurannya yang tebalnya hanya setengah dari PC card tipe III.

   Mykotronx Corp.

   Perusahaan Mykotronx membuat token Fortezza card untuk penggunaan laptop yang dilengkapi dengan PC card.

4. Smart Card

   Smart card lebih murah jika dibandingkan dengan token-token bentuk lainnya. Smart card juga memiliki kemungkinan yang besar untuk berumur pendek karena gesekan ketika memasukkan kartu potensial dapat memperpendek umur dari token smart card.

5. Universal Serial Bus (USB)

   USB telah menjadi standard dalam komputer saat ini. Token USB karenanya menjadi alternatif yang lebih murah dibandingkan token-token lainnya yang membutuhkan alat input khusus.

   Booleansoft

   Booleansoft mempunyai beberapa tipe token-token USB, beberapa diantaranya termasuk biometrik sidik jari. Setiap client yang meminta autentikasi aman disediakan melalui token keamanan pribadi.

   Ketika token USB dimasukkan ke dalam port USB komputer, sebuah program software yang disimpan dalam token secara otomatis dijalankan. Software token mengijinkan user menggenerate one-tim password baru dan digital signature untuk mengakses resource terpisah untuk tujuan autentikasi.

   Verisign

   Verisign Unified Authentication menyediakan platform tunggal terintegrasi untuk merencanakan dan mengatur seluruh tipe dari autentikasi dua faktor.

6. Token USB berbasis smart card

   Token USB berbasis smart card mengandung sebuah chip smart card didalamnya yang menyediakan fungsionalitas token USB dan smart card. Token ini memungkinkan solusi keamanan skala besar dan menyediakan kemampuan dan keamanan dari smart card tradisional tanpa membutuhkan alat input khusus.

   Dari sudut pandang sistem operasi komputer, token ini merupakan USB connected smart card reader dengan satu smart card tetap.

7. Model lainnnya

   Beberapa menggunakan antarmuka khusus, contohnya crypto ignition key yang dibuat oleh National Security Agency (NSA) Amerika Serikat. Token juga dapat digunakan sebagai kartu identitas. Telepon genggam dan PDA juga dapat berfungsi sebagai

security token dengan pemrograman seperlunya.

Penggunaan security token

Security token yang paling sederhana tidak memerlukan koneksi apapun ke sebuah komputer. Client memasukkan nomer yang ditampilkan pada token yang dimilikinya, biasanya dengan menggunakan PIN. Token lainnya dihubungkan dengan komputer menggunakan teknik wireless seperti bluetooth.

Terakhir dengan menghubungkannya langsung ke komputer melalui alat input yang sesuai. Untuk tipe yang terakhir, sistem operasi komputer dapat membaca kunci yang diberikan oleh token dan melaksanakan operasi kriptografi padanya atau dapat juga meminta firmware token untuk menjalankan operasinya.

4. Teknologi terkait dengan security token

Two-factor Authentication

Two-factor authentication adalah protokol autentikasi yang membutuhkan dua cara independen untuk menciptakan identitas dan hak istimewa. Hal ini sangat bertentangan dengan autentikasi passsword tradisional yang memerlukan hanya satu faktor (pengetahuan dari nilai password) untuk memperoleh akses ke sistem

Implementasi umum dari two-factor authentication menggunakan ‘sesuatu yang Anda tahu’ (contohnya password atau PIN) sebagai satu dari dua faktor, dan menggunakan antara ‘sesuatu yang Anda miliki’ (alat fisik seperti telepon selular, kartu kredit, atau security token) atau ‘sesuatu yang adalah Anda’ (contohnya biometrik seperti sidik jari, scan retina mata, dan biometrik lainnya) sebagai faktor lainnya.

Contoh umum dari two-factor authentication adalah kartu bank (kartu kredit atau kartu debit), dimana kartu itu sendiri merupakan alat fisik ‘sesuatu yang Anda miliki’ dan PIN yang sesuai merupakan password ‘sesuatu yang Anda tahu’. Menggunakan lebih dari satu faktor disebut juga autentikasi kuat, sehingga menggunakan hanya satu faktor saja (seperti contoh hanya password statis) dapat disebut juga sebagai autentikasi lemah. Autentikasi kuat juga termasuk multi faktor dimana tidak termasuk faktor fisik (kartu atau alat).

Berdasarkan anjuran-anjuran, two-factor authentication dapat secara drastis mengurangi insiden pencurian data identitas online dan kejahatan online lainnya, karena password dari korban tidak lagi cukup untuk memberikan pencurinya akses ke informasi korban. Namun bagaimanapun juga, two-factor authentication masih rawan terhadap program trojan dan serangan man-in-the-middle.

Penyebaran dari alat-alat two-factor authentication seperti smart card dan token USB tambaak semakin bertambah. Semakin banyak organisasi yang telah menambahkan lapisan keamanan baru yang membutuhkan user untuk memiliki secara fisik sebuah token, dan mempunyai pengetahuan tentang PIN atau password untuk dapat mengakses data organisasi.

Namun, masih terdapat beberapa kekurangan pada two-factor authentication yang menyebabkan teknologi ini belum berkembang luas. Beberapa customer mengalami kesulitan menjaga agar tidak hilang satu atau lebih barang-barang yang dimilikinya. Selain itu, banyak solusi two-factor authentication yang dimiliki dan dilindungi oleh paten. Akibatnya adalah biaya tahunan yang besar per orang yang dilindungi oleh two-factor authentication dan kurangnya interoperabilitas.

5. Implementasi Security Token Pada Token PIN Mandiri

Token PIN Mandiri adalah alat pengaman tambahan untuk transaksi finansial di Elektronik Banking Bank Mandiri. Token

PIN Mandiri berfungsi untuk menghasilkan PIN yang selalu berganti (PIN Dinamis) untuk setiap kali nasabah melakukan transaksi finansial. PIN Dinamis tersebut disebut juga PIN Mandiri.

PIN Mandiri dapat digunakan saat bertransaksi di salah satu Channels Elektronik Banking Bank Mandiri yaitu, Internet Banking Mandiri, SMS Banking Mandiri dan Call Mandiri. Saat ini Token PIN Mandiri baru bisa digunakan di Internet Banking Mandiri

Gambar 7. Token PIN Mandiri

Penggunaan Tombol Token PIN Mandiri

Fungsi Tombol 1, 2, dan 3, pada saat layar menu pada posisi 'APPLI –' adalah tombol pilihan metoda yang dapat digunakan:

1. Pilihan Tombol 1 (Metoda APPLI 1) bila diminta menggunakan metoda yang mengharuskan input data terlebih dahulu (challenge number) untuk bisa mendapatkan nomor PIN Mandiri.
   Contoh: pada saat bertransaksi.

2. Pilihan Tombol 2 (Metoda APPLI 2) bila diminta menggunakan metoda yang langsung mengeluarkan nomor PIN Mandiri.
   Contoh: Aktivasi Token PIN Mandiri.

3. Pilihan Tombol 3 (Metoda APPLI 3) bila diminta menggunakan metoda yang mengharuskan input 3 data terlebih dahulu (3 chalenge number) untuk bisa mendapatkan nomor PIN Mandiri.

4. Tombol Merah adalah tombol multifungsi yang berguna untuk:

   a. Mengaktifkan atau menonaktifkan Token PIN Mandiri.
   b. Menjadi tombol "Backspace" pada saat sedang melakukan input data.
   c. Untuk merubah Password Token PIN Mandiri bila ditekan selama 3 detik, saat layar menu pada posisi 'APPLI –'.
   d. Untuk kembali ke menu utama setelah PIN Mandiri dihasilkan.

Untuk bisa bertransaksi dengan menggunakan Token PIN Mandiri tersebut customer diharuskan untuk segera melakukan penggantian password Token PIN Mandiri dan aktivasi Token PIN Mandiri di Internet Banking Mandiri menu administrasi

Penggunaan Token PIN Mandiri

Beberapa contoh penggunaan Token PIN Mandiri dalam bertransaksi Elektronik Banking di Bank Mandiri antara lain:

a. Mengganti Password Token PIN Mandiri pertama Kali

   1. Aktifkan Token PIN Mandiri dengan menekan tombol merah pada keypad
   2. Pada layar Token PIN Mandiri akan tampil: PIN _ _ _ _ _ _ _ _
   3. Masukkan Password awal Token PIN Mandiri, yaitu 12345678
   4. Pada layar akan tampil: NEW PIN _ _ _ _ _ _

5. Masukkan Password baru Token PIN Mandiri sesuai yang dikehendaki
6. Pada layar akan tampil: PIN CONF _ _ _ _ _ _
7. Masukkan Password baru sekali lagi
8. Jika benar pada layar akan tampil NEW PIN CONF dan selanjutnya akan masuk ke menu: APPLI -
9. Tekan tombol merah sekali lagi jika ingin mematikan Token PIN Mandiri
10. Proses perubahan Password Token PIN Mandiri pertama kali telah selesai

b. Melakukan Aktivasi Token PIN Mandiri

Pada Layar Komputer:

1. Login ke Internet Banking Mandiri dengan menggunakan USER ID dan PIN Internet Banking Mandiri
2. Pilih Menu “Administrasi”
3. Pilih “Aktivasi Token PIN Mandiri”

Pada Token PIN Mandiri:

4. Aktifkan Token PIN Mandiri dengan menekan tombol merah pada keypad
5. Pada layar Token PIN Mandiri akan ter-display : PIN _ _ _ _ _ _
6. Masukan 6 digit angka password Token PIN Mandiri
7. Pada layar akan ter-display: APPLI
8. Tekan angka 2 (dua) pada keypad (Metoda APPLI 2) dan pada layar Token PIN Mandiri akan tampil 6 digit nomor PIN Mandiri

Pada Layar Komputer:

9. Masukkan 6 digit Nomor PIN Mandiri tersebut pada kolom “Masukkan PIN Mandiri Anda untuk Aktivasi” di layar komputer
10. Tekan tombol “KIRIM”

Pada Token PIN Mandiri:

11. Tekan Tombol merah untuk kembali ke menu APPLI
12. Tekan Tombol merah sekali lagi jika ingin mematikan Token PIN Mandiri
13. Proses Aktivasi Token PIN Mandiri telah selesai

c. Melakukan Transaksi dengan menggunakan Token PIN Mandiri

Pada Token PIN Mandiri:

1. Aktifkan Token PIN Mandiri dengan menekan tombol merah pada keypad
2. Pada layar Token PIN Mandiri akan ter-display : PIN _ _ _ _ _ _
3. Masukan 6 digit angka password Token PIN Mandiri
4. Pada layar akan ter-display: APPLI
5. Tekan angka 1 (satu) pada keypad (Metoda APPLI 1) dan pada layar Token PIN Mandiri akan tampil : _ _ _ _ _ _ _ _ _ _

Pada Layar Komputer:

6. Lihat angka yang terdapat di kolom “Challenge Code” pada layar konfirmasi Internet Banking Mandiri

Pada Token PIN Mandiri:

7. Masukkan seluruh angka yang terdapat pada kolom “Challenge Code” di layar komputer ke Token PIN Mandiri
8. Kemudian tekan tombol merah selama 3 detik hingga layar pada Token PIN Mandiri berubah
9. Pada layar Token PIN Mandiri anda akan tampil 6 digit nomor PIN Mandiri

Pada Layar Komputer Anda:

10. Masukkan 6 digit Nomor PIN Mandiri tersebut pada layar konfirmasi Internet Banking Mandiri di kolom “Masukkan

PIN Mandiri Anda untuk Konfirmasi”

11. Tekan tombol “kirim” setelah memeriksa seluruh data konfirmasi

Pada Token PIN Mandiri:

12. Tekan Tombol merah untuk kembali ke menu APPLI
13. Atau tekan Tombol merah sekali lagi jika ingin mematikan Token PIN Mandiri
14. Proses Transaksi dengan menggunakan Token PIN Mandiri telah selesai

d. Merubah Password Token PIN Mandiri

1. Aktifkan Token PIN Mandiri dengan menekan tombol merah pada keypad
2. Pada layar Token PIN Mandiri akan tampil : PIN _ _ _ _ _ _ _ _
3. Masukkan 6 digit angka Password Token PIN Mandiri
4. Pada layar akan ter-display: APPLI
5. Kemudian tekan tombol merah selama 3 detik hingga layar pada Token PIN Mandiri berubah.
6. Pada layar akan tampil : NEW PIN _ _ _ _ _ _
7. Masukkan Password baru Token PIN Mandiri sesuai yang dikehendaki
8. Pada layar akan tampil: PIN CONF _ _ _ _ _ _
9. Masukkan Password baru sekali lagi
10. Jika benar Pada layar akan tampil NEW PIN CONF dan layar akan kembali ke menu: APPLI
11. Tekan tombol merah sekali lagi jika ingin mematikan Token PIN Mandiri
12. Proses perubahan Password Token PIN Mandiri telah selesai

e. Membuka Token PIN Mandiri yang terkunci

Customer Service Bank Mandiri:

1. Customer Service Bank Mandiri akan meminta nomor challenge yang terdapat pada Token PIN Mandiri

Pada Token PIN Mandiri:

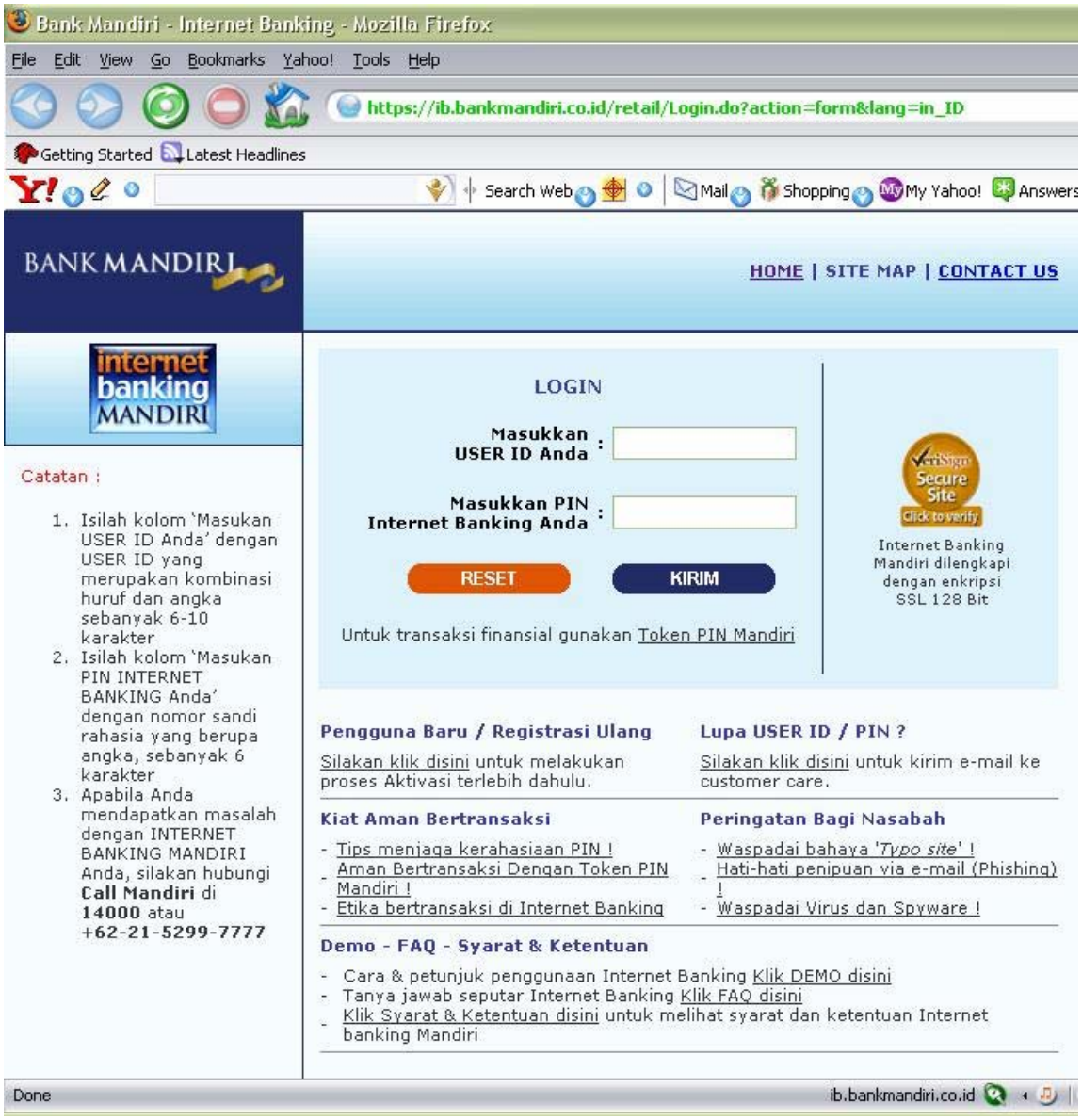
2. Aktifkan Token PIN Mandiri dengan menekan tombol merah pada keypad
3. Pada layar Token PIN Mandiri akan tampil: LOCK PIN xxxxxxx (xxxxxxx adalah 7 digit nomor challenge), sebutkan 7 digit nomor tersebut kepada Customer Service Bank Mandiri.

Customer Service Bank Mandiri:

4. Customer Service Bank Mandiri akan menerima dan memasukkan nomor tersebut ke dalam sistem.
5. Selanjutnya Customer Service Bank Mandiri akan memberikan nomor response yang keluar dari sistem

Pada Token PIN Mandiri:

6. Pada posisi layar: LOCK PIN xxxxxx , Tekan tombol merah pada keypad.
7. Pada layar akan tampil : LOCK PIN _ _ _ _ _ _ _ _
8. Masukkan 8 digit angka response yang diberikan oleh Customer Service Bank Mandiri.
9. Pada layar akan tampil : NEW PIN _ _ _ _ _ _
10. Masukkan Password baru Token PIN Mandiri sesuai yang dikehendaki
11. Pada layar akan tampil: PIN CONF _ _ _ _ _ _
12. Masukkan Password baru sekali lagi
13. Proses membuka Token PIN Mandiri yang terkunci selesai.



Gambar 8. Halaman Website Internet Banking Bank Mandiri

Sinkronisasi

Bila Token PIN Mandiri terlalu lama tidak digunakan bertransaksi dan pada saat bertransaksi sistem tidak menerima angka PIN Mandiri yang dimasukkan maka harus dilakukan sinkronisasi dengan cara menghubungi Call Mandiri atau Cabang Bank Mandiri Terdekat.

Teknologi Token PIN Mandiri

Token yang digunakan oleh Bank Mandiri adalah yang diproduksi oleh VASCO yaitu jenis DigiPass 260. DigiPass adalah produk sekuriti dari VASCO yang menyediakan autentikasi kuat user dan e-signature via security token kecil yang dibawa oleh user. DigiPass kompatibel dengan lebih dari 50 vendor internasional untuk kebutuhan e-commerce, e-banking, e-networking dan aplikasi e-government.

Token ini bekerja berdasarkan waktu (time base) dimana server token ini ditempatkan. Bank Mandiri menggunakan server autentikasi Velis Authenticator (VA).

Masing-masing token memiliki secred/ seed value yang unik, dimana masing-masing token ini memiliki value yang berbeda. secred/ seed value ini adalah sebagai variabel dasar yang nantinya akan dikombinasikan dengan variable lainya untuk menghasilnya password/ PIN dalam suatu satuan waktu.

Aplikasi yang terdapat di dalam token DigiPass 260 ada tiga buah, yaitu:

1. Aplikasi Response Only (RO)

   Aplikasi ini memiliki dua variable yaitu, secred/seed value dan time (waktu saat ini), untuk menggenerate password/ PIN.

2. Aplikasi Challenge Response (C/R)

   Aplikasi ini memiliki tiga variable yaitu, secred/seed value dan time (waktu saat ini) dan challenge yaitu berupa angka dengan digit tertentu yang digenerate oleh server VA yang harus di input ke dalam token, untuk menggenerate password/ PIN.

   Salah satu fungsi dari aplikasi C/R ini adalah untuk menghindari jebakan pada website palsu (phishing), seperti yang pernah terjadi pada klikBCA milik bank BCA. Karena website tersebut tidak mungkin menampilkan angka challenge dari server VA.

3. Aplikasi Digital Signature

   Aplikasi ini mirip dengan C/R, hanya saja challenge yang disediakan lebih dari satu challenge (maksimal delapan) yang dapat diinputkan ke dalam token. 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 oleh Bank Mandiri adalah tiga buah. Field pertama adalah nomer rekening pengirim, field kedua adalah nomer rekening tujuan, dan field terakhir adalah nominal tranfer. Ketiga field ini dikombinasikan dengan secret/seed value dan time, akan menghasilkan PIN/ password.

Token VASCO menggunakan teknologi time window, yaitu server VA masih dapat mengenali beberapa value Password/ PIN yang digenerate pada beberapa interval waktu sebelumnya oleh token.

Token VASCO ini diinisialisasi dengan algoritma dengan parameter tertentu, yang dikerjakan oleh software DigiPass Programmer. Pada software DigiPass Programmer ini operator dapat menentukan PIN length, challenge length, initial token PIN, jumlah aplikasi yang digunakan, jenis aplikasi yang digunakan, penanganan error PIN dan sebagainya.

Output dari software ini ada dua yaitu, initialized token dan file .dpx, yaitu informasi mengenai algoritma dan parameter yang digunakan token termasuk waktu yang digunakan pada saat token diinitialize dan juga serial number token dan sebagainya.

Token ini dapat berkomunikasi dengan internet banking. Kuncinya adalah pada file *.dpx tadi. File tersebut di upload/ export ke dalam server VA. Dengan ini server VA akan mengenali bahwa ada sejumlah n token, yang masing-masing token memiliki parameter dan algoritma sekian. Kemudian server VA akan melakukan proses assignment terhadap masing-masing token kepada user yang menggunakan token tersebut.

Lalu server VA akan berkomunikasi dengan server Internet Banking. Ketika seorang user mencoba login maka, ID dan PIN yang diinput olehnya akan dikirim ke server VA oleh Internet Banking. Server VA hanya akan memberikan dua jawaban, yaitu accepted atau rejected. Kemudian informasi ini akan dikembalikan kepada Internet Banking untuk transaksi berikutnya.

6. Kesimpulan

Dari pembahasan di atas mengenai manajemen kunci kriptografi dengan security token dan implementasinya pada token PIN Mandiri dapat ditarik beberapa kesimpulan:

1. Internet Banking masih belum cukup aman bagi customer karena banyak celah-celah yang dapat diserang, contohnya dengan phishing, pharming, serangan man-in-the-middle, dan lain-lain.

2. Salah satu pengamanan Internet Banking yang sangat baik adalah dengan menggunakan manajemen kunci kriptografi dengan security token yang dapat menggenerate password (dynamic password).

3. Salah satu security token yang baik namun tetap efisien adalah security token one-time password berbasis sinkronisasi waktu dengan two-ways authentication (atau lebih).

4. Salah satu bank di Indonesia yang telah menggunakan teknologi internet banking adalah Bank Mandiri yang menggunakan token PIN Mandiri sebagai salah satu lapisan pengamanannya.

5. Token PIN Mandiri merupakan teknologi DigiPass 260 paten milik VASCO yang cukup handal dan teruji keamanannya.

6. Selain pengamanan dengan token PIN Mandiri, customer internet banking tetap harus selalu waspada dengan selalu menjaga password security token yang dimilikinya dan selalu berhati-hati ketika melakukan transaksi internet banking.

Daftar Pustaka

[1] Bank Mandiri - Aman Bertransaksi Dengan Token PIN Mandiri http://www.bankmandiri.co.id/article/securitytips.aspx?id=FFAN20461035 Tanggal akses: 14 Desember 2006 pukul 22:00.

[2] Bank Mandiri - Internet Banking Mandiri, Aman dari 'Keylogger' http://www.bankmandiri.co.id/article/securitytips.aspx?id=FFAN35037802 Tanggal akses: 14 Desember 2006 pukul 22:00.

[3] Buku Petunjuk Penggunaan Token PIN Mandiri. Bank Mandiri. 2006

[4] Los Alamos National Bank (US) Selects VASCO's Digipass 260 and GO3 to Secure its Corporate Clients http://www.lexdon.com/article/los_alamos_national_bank_(us)/61784.html Tanggal akses: 14 Desember 2006 pukul 22:00.

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

[6] Teknologi Token KlikBCA/Mandiri
http://www.pakarkomputer.com/node/55
Tanggal akses: 14 Desember 2006 pukul 22:00.

[7] Two Factor Authentication Solution with VASCO DigiPass Tokens for Internet Banking
http://www.i-sprint.com/solutions_2fa.htm
Tanggal akses: 14 Desember 2006 pukul 22:00.

[8] VASCO
http://www.vasco.com/
Tanggal akses: 14 Desember 2006 pukul 22:00.

[9] VASCO ABN AMRO
http://www.vasco.com/documents/customers/casestudies/VASCO_ABN_AMRO.pdf
Tanggal akses: 14 Desember 2006 pukul 22:00.

[10] VASCO - Digipass Pro 260
http://www.vasco.com/products/product.html?product=49
Tanggal akses: 14 Desember 2006 pukul 22:00.

[11] VelisSoftware - VelisAssetManager
http://www.velissoftware.com/index.php?p=product_vam
Tanggal akses: 14 Desember 2006 pukul 22:00.

[12] Why use VASCO Digipass Strong Authentication & Signatures?
http://www.vasco.com/ebanking.html
Tanggal akses: 14 Desember 2006 pukul 22:00.

[13] WIKIPEDIA – One-Time Password
http://en.wikipedia.org/wiki/One-time_password
Tanggal akses: 14 Desember 2006 pukul 22:00.

[14] WIKIPEDIA – Security Token
http://en.wikipedia.org/wiki/Security_token
Tanggal akses: 14 Desember 2006 pukul 22:00.

[15] WIKIPEDIA – Two-Factor Authentication
http://en.wikipedia.org/wiki/Two-factor_authentication
Tanggal akses: 14 Desember 2006 pukul 22:00.