Keamanan Sistem WWW

WWW security

Sejarah WWW

- Dikembangan oleh Tim Berners-Lee ketika sedang berada di CERN
- Kemudahan untuk mengakses informasi melalui sistem hypertext
- Mula-mula dikembangkan di lingkungan sistem operasi NeXT, kemudian muncul program Mosaic (Windows, Mac, Unix, multiplatform), dan … akhirnya Netscape. Kemudian meledak

Sejarah WWW

- Bahan bacaan
  - http://ensiklomedia.insan.co.id
  - Buku Tim Berners-Lee, “Weaving the Web”
  - http://www.w3.org

Peta Perjalanan WWW

- Memungkinkan untuk mengimplementasikan sistem secara tersentralisasi
  - Client hanya membutuhkan web browser (yang ada di semua komputer), thin client
  - Update software bisa dilakukan di server saja, tanpa perlu mengubah sisi client
  - Browser di sisi client dapat ditambah dengan “plugin” untuk menambahkan fitur (animasi, streaming audio & video); Macromedia Flash / Shockwave
  - Mulai banyak aplikasi yang menggunakan basis web
- Aplikasi baru
  - Blog
  - Authentication

Sistem WWW

- Arsitektur sistem WWW
  - Server (apache, IIS)
  - Client
    - IE, Firefox, Netscape, Mozilla, Safari, Opera, Galeon, kfm, arena, amaya, lynx, K-meleon
  - Terhubung melalui jaringan
- Program dapat dijalankan di server (CGI, [java] servlet) atau di sisi client (javascript, java applet)

Asumsi [Sisi Pengguna]

- Server dimiliki dan dikendalikan oleh organisasi yang mengaku memiliki server tersebut
- Dokumen yang ditampilkan bebas dari virus atau itikad jahat lainnya
- Server tidak mencatat atau mendistribusikan informasi tentang user (misalnya kebiasaan browsing)

Asumsi [Sisi Webmaster]

- Pengguna tidak beritikad untuk merusak web server atau mengubah isinya
- Pengguna hanya mengakses dokumen[2] yang diperkenankan diakses (dimana dia memiliki ijin)
- Identitas pengguna benar

Asumsi Kedua Pihak

- Network dan komputer bebas dari penyadapan pihak ketiga
- Informasi yang disampaikan dari server ke pengguna (dan sebaliknya) terjamin keutuhannya dan tidak dimodifikasi oleh pihak ketiga

Keamanan Server WWW

- Server WWW (httpd) menyediakan informasi (statis dan dinamis)
- Halaman statis diperoleh dengan perintah GET
- Halaman dinamis diperoleh dengan
  - CGI (Common Gateway Interface)
  - Server Side Include (SSI)
  - Active Server Page (ASP), PHP
  - Servlet (seperti Java Servlet, ASP)

Eksploitasi server WWW

- Tampilan web diubah (*deface*)
  - dengan eksploitasi skrip / previledge / OS di server
  - Situs yang dideface dikoleksi di http://www.alldas.org, http://www.zone-h.org
- Data di server berubah
  - Masuk ke server dan mengubah secara manual
  - Mengubah data melalui CGI (akan dibahas kemudian)
  - Mengubah data di database (SQL injection, XSS)
- Informasi bocor
  - Contoh, laporan keuangan semestinya hanya dapat diakses oleh orang/ bagian tertentu

Eksploitasi server WWW [2]

- Penyadapan informasi
  - URLwatch: melihat siapa mengakses apa saja. Masalah privacy
  - SSL memproteksi, namun tidak semua menggunakan SSL karena komputasi yang tinggi
- DoS attack
  - Request dalam jumlah yang banyak (bertubi-tubi)
  - Request yang memblokir (lambat mengirimkan perintah GET)

Eksploitasi server WWW [3]

- Digunakan untuk menipu firewall (*tunelling* ke luar jaringan)
- Port 80 digunakan untuk identifikasi server (karena biasanya dibuka di router/firewall)
  - telnet ke port 80 (dibahas di bagian lain)

Membatasi Akses

- Access Control
  - Hanya IP tertentu yang dapat mengakses server (konfigurasi web server atau firewall)
  - Via userid & password (htaccess)
  - Menggunakan token
  - Menggunakan enkripsi untuk menyandikan data-data

htaccess di Apache

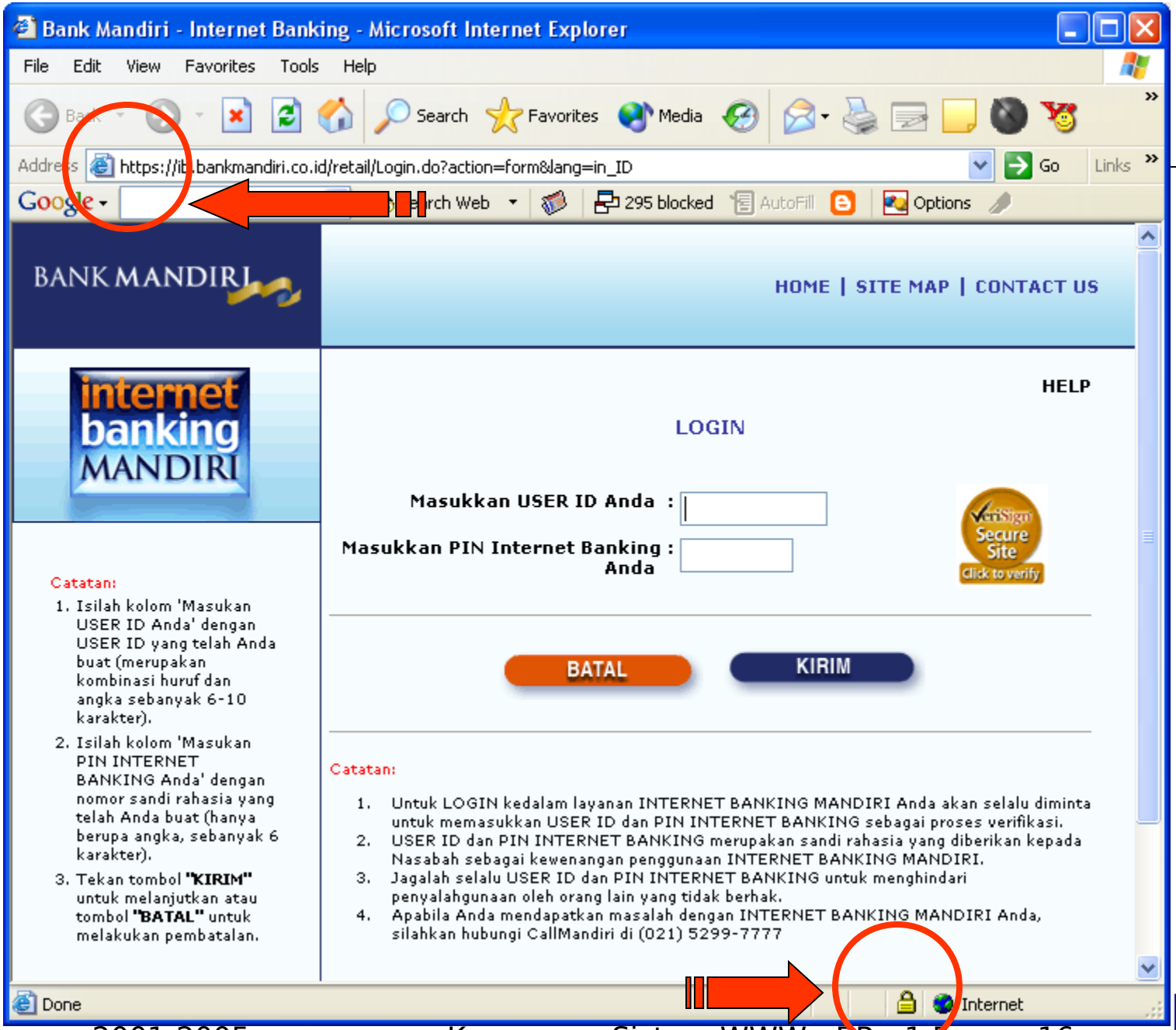
- Isi berkas "`.htaccess`"

```
AuthUserFile /home/budi/.passme
AuthGroupFile /dev/null
AuthName "Khusus untuk Tamu Budi"
AuthType Basic
<Limit GET>
    require user tamu
</Limit>
```

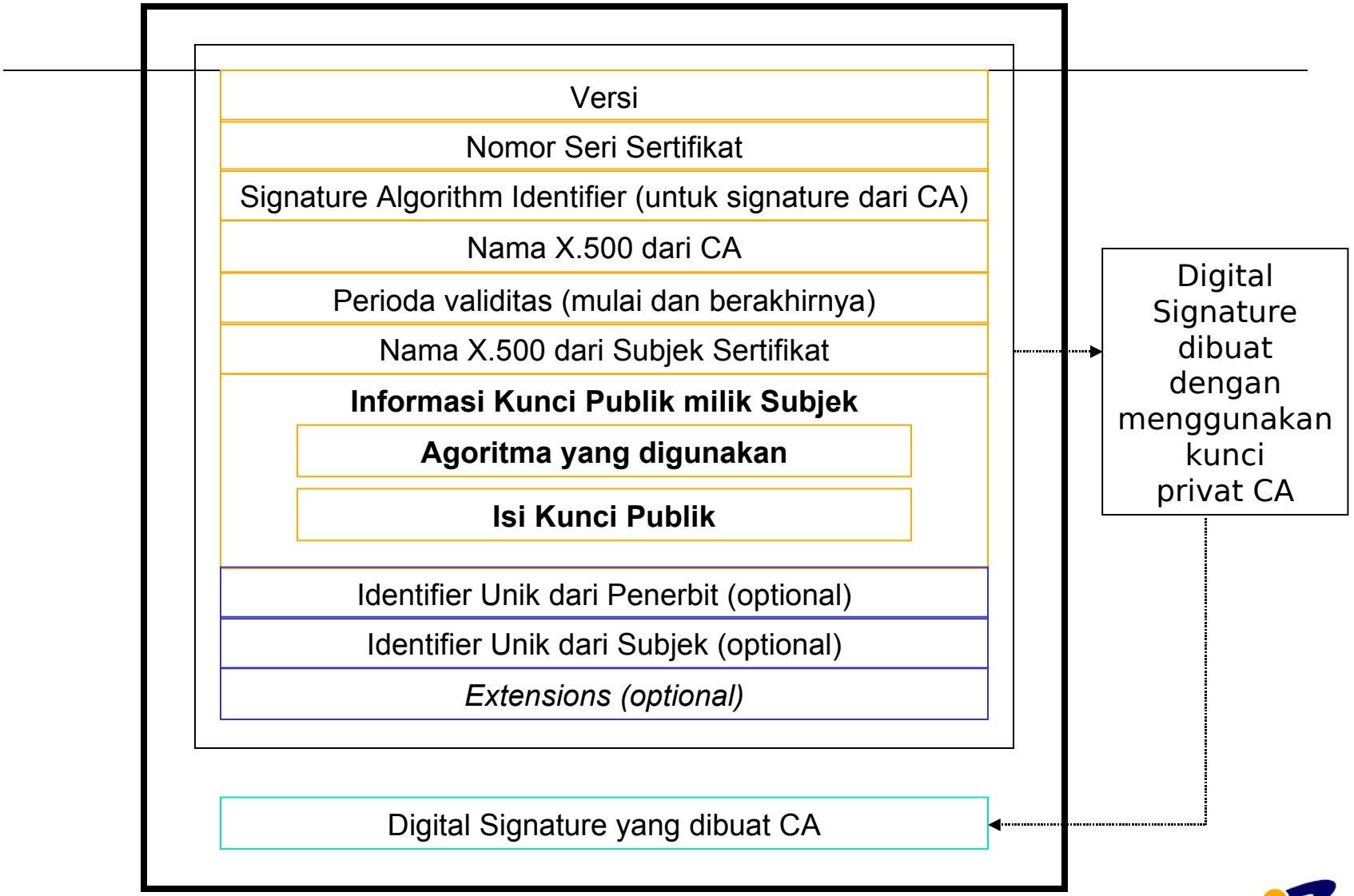
- Membatasi akses ke user "tamu" dan password
- Menggunakan perintah "`htpasswd`" untuk membuat password yang disimpan di ".passme"

Secure Socket Layer (SSL)

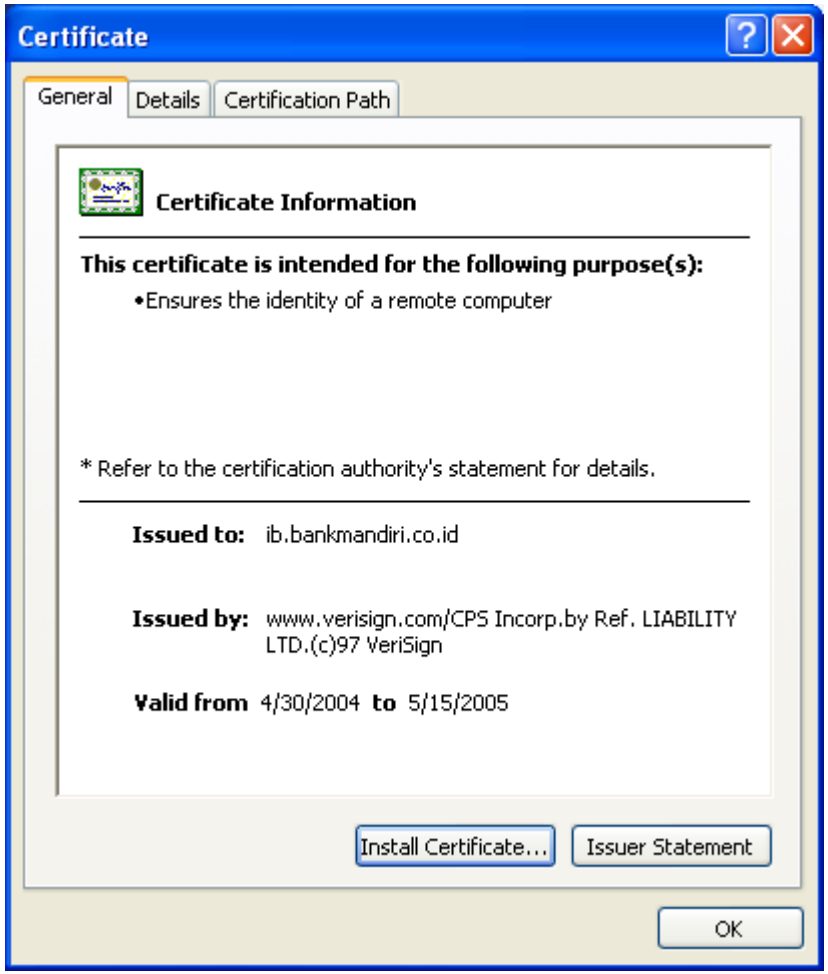
- Menggunakan enkripsi untuk mengamankan transmisi data
- Mulanya dikembangkan oleh Netscape
- Implementasi gratis pun tersedia
  - openSSL
- Beberapa masalah dengan SSL
  - ASN.1 compiler yang bermasalah menimbulkan masalah di beberapa implementasi SSL (sehingga server down)

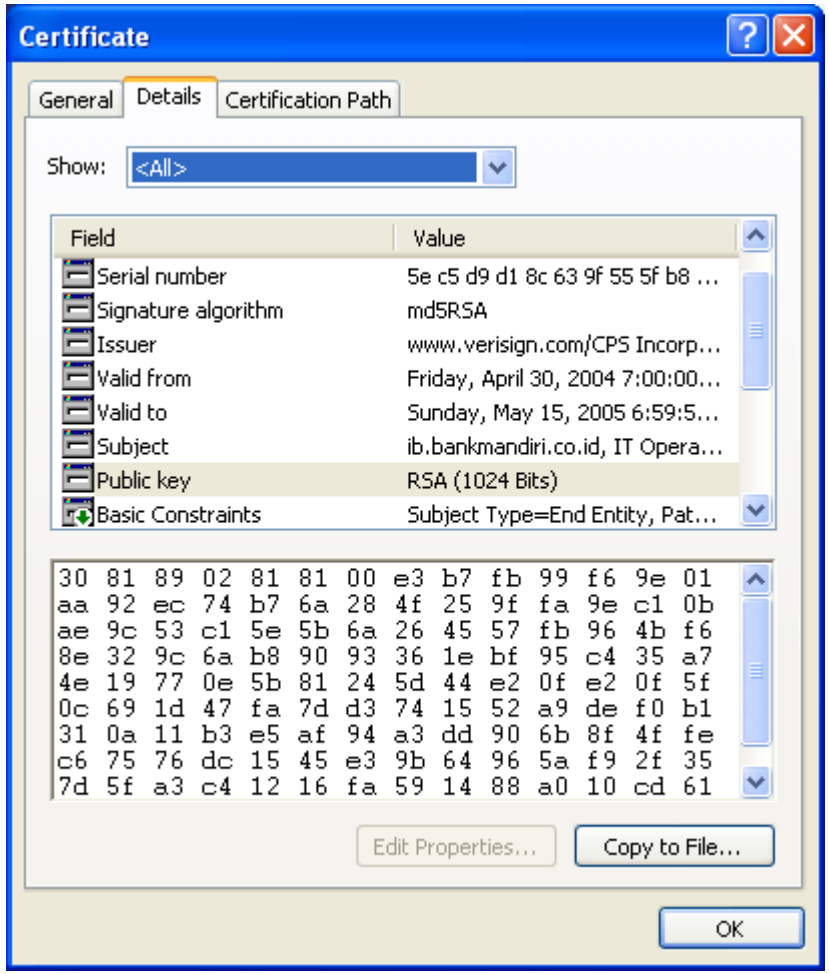

Bank Mandiri - Internet Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites Media
Address https://ib.bankmandiri.co.id/retail/Login.do?action=form&lang=in_ID
Go Links
Google
295 blocked AutoFill Options
BANK MANDIRI
HOME | SITE MAP | CONTACT US
internet banking MANDIRI
HELP
LOGIN
Masukkan USER ID Anda :
Masukkan PIN Internet Banking : Anda
VeriSign Secure Site Click to verify
BATAL
KIRIM
Catatan:
1. Isilah kolom 'Masukan USER ID Anda' dengan USER ID yang telah Anda buat (merupakan kombinasi huruf dan angka sebanyak 6-10 karakter).
2. Isilah kolom 'Masukan PIN INTERNET BANKING Anda' dengan nomor sandi rahasia yang telah Anda buat (hanya berupa angka, sebanyak 6 karakter).
3. Tekan tombol "KIRIM" untuk melanjutkan atau tombol "BATAL" untuk melakukan pembatalan.
Catatan:
1. Untuk LOGIN kedalam layanan INTERNET BANKING MANDIRI Anda akan selalu diminta untuk memasukkan USER ID dan PIN INTERNET BANKING sebagai proses verifikasi.
2. USER ID dan PIN INTERNET BANKING merupakan sandi rahasia yang diberikan kepada Nasabah sebagai kewenangan penggunaan INTERNET BANKING MANDIRI.
3. Jagalah selalu USER ID dan PIN INTERNET BANKING untuk menghindari penyalahgunaan oleh orang lain yang tidak berhak.
4. Apabila Anda mendapatkan masalah dengan INTERNET BANKING MANDIRI Anda, silahkan hubungi CallMandiri di (021) 5299-7777
Done
Internet

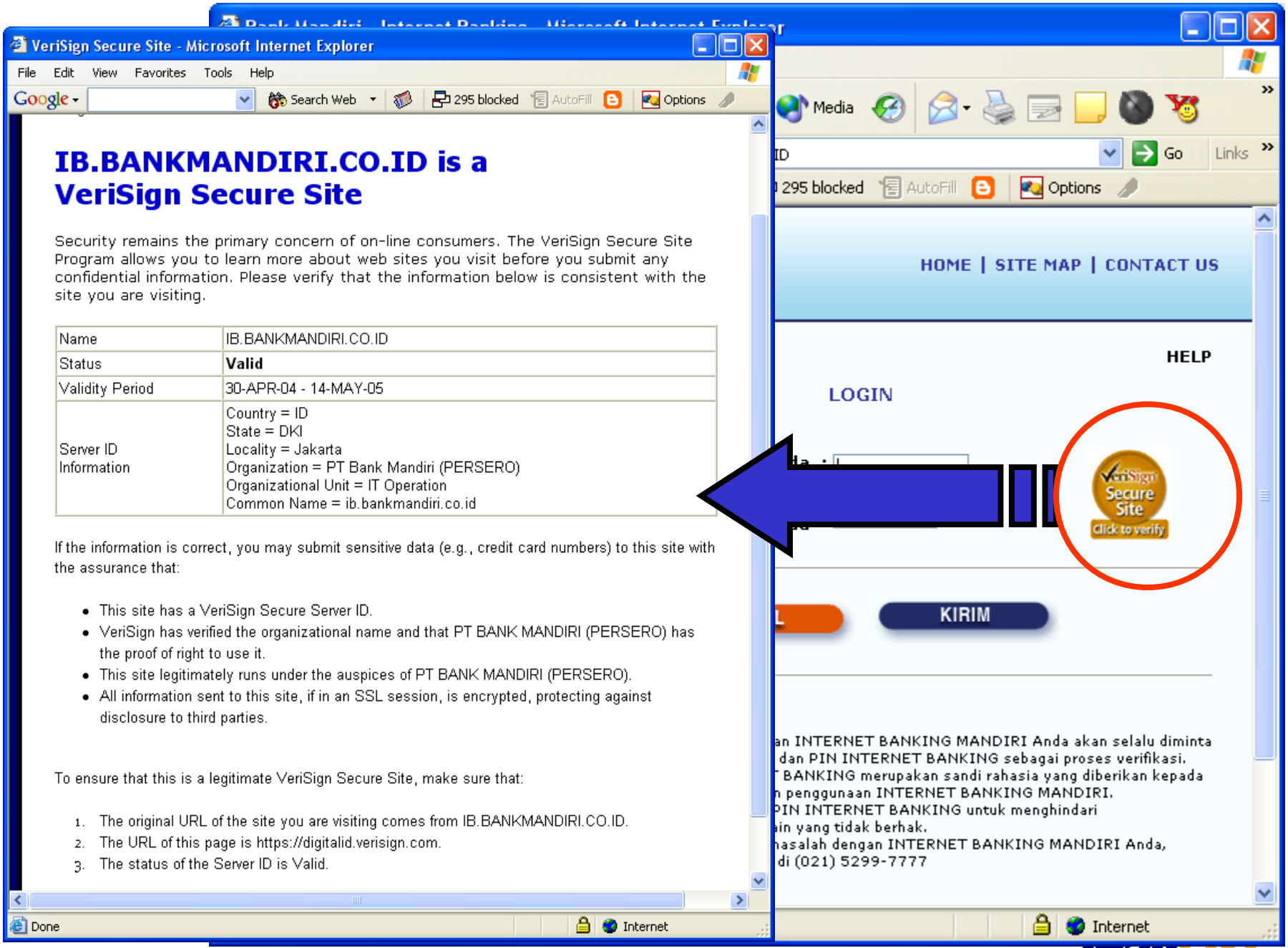
Sertifikat X.509 versi 3



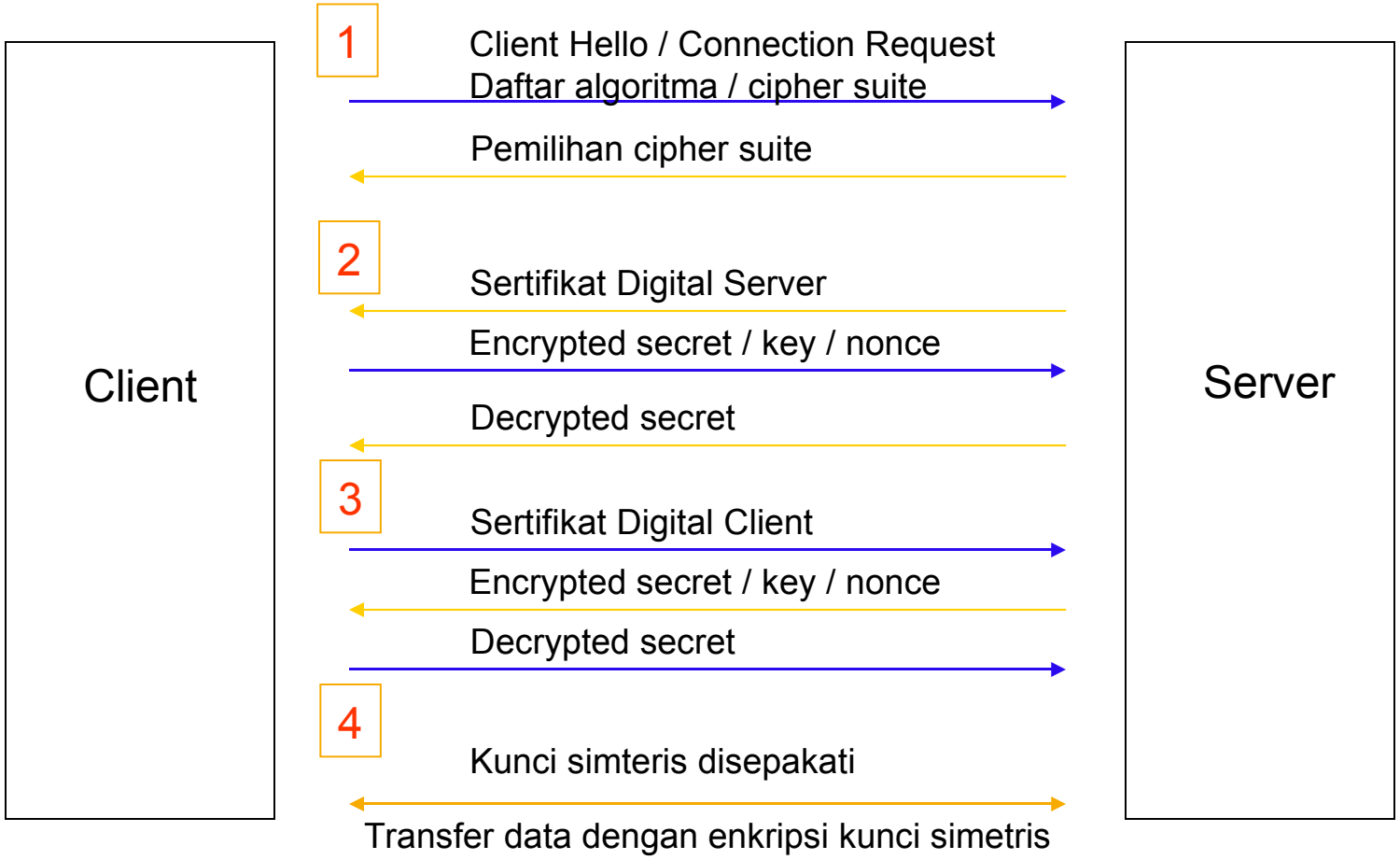
Contoh Sertifikat






VeriSign Secure Site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Google
Search Web
295 blocked
AutoFill
Options
IB.BANKMANDIRI.CO.ID is a VeriSign Secure Site
Security remains the primary concern of on-line consumers. The VeriSign Secure Site Program allows you to learn more about web sites you visit before you submit any confidential information. Please verify that the information below is consistent with the site you are visiting.
Name
IB.BANKMANDIRI.CO.ID
Status
Valid
Validity Period
30-APR-04 - 14-MAY-05
Server ID Information
Country = ID
State = DKI
Locality = Jakarta
Organization = PT Bank Mandiri (PERSERO)
Organizational Unit = IT Operation
Common Name = ib.bankmandiri.co.id
If the information is correct, you may submit sensitive data (e.g., credit card numbers) to this site with the assurance that:
This site has a VeriSign Secure Server ID.
VeriSign has verified the organizational name and that PT BANK MANDIRI (PERSERO) has the proof of right to use it.
This site legitimately runs under the auspices of PT BANK MANDIRI (PERSERO).
All information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties.
To ensure that this is a legitimate VeriSign Secure Site, make sure that:
1. The original URL of the site you are visiting comes from IB.BANKMANDIRI.CO.ID.
2. The URL of this page is https://digitalid.verisign.com.
3. The status of the Server ID is Valid.
Done
Internet
Media
Go
Links
295 blocked
AutoFill
Options
HOME | SITE MAP | CONTACT US
HELP
LOGIN
VeriSign Secure Site Click to verify
KIRIM
an INTERNET BANKING MANDIRI Anda akan selalu diminta
dan PIN INTERNET BANKING sebagai proses verifikasi.
BANKING merupakan sandi rahasia yang diberikan kepada
penggunaan INTERNET BANKING MANDIRI.
PIN INTERNET BANKING untuk menghindari
in yang tidak berhak.
asalah dengan INTERNET BANKING MANDIRI Anda,
di (021) 5299-7777
Internet

Protokol SSL



Cari info server

- Informasi tentang server digunakan sebagai bagian dari casing the joint
- Dapat dilakukan dengan
  - Memberikan perintah HTTP langsung via telnet
  - Menggunakan program netcat

Keamanan CGI

- Pada mulanya CGI digunakan sebagai *interface* dengan sistem informasi lainnya (gopher, WAIS, ftp)
- Diimplementasikan dengan berbagai bahasa (perl, C, C++, python, sh, dll.)
- Skrip CGI dijalankan di server (oleh siapa saja dari jaringan) sehingga membuka potensi lubang keamanan jika skrip tidak dibuat dengan baik

Lubang Keamanan CGI

- Beberapa contoh
  - CGI dipasang oleh orang yang tidak berhak
  - CGI dijalankan berulang-ulang untuk menghabiskan resources (CPU, disk): DoS
  - Masalah *setuid* CGI di sistem UNIX, dimana CGI dijalankan oleh userid web server
  - Penyisipan karakter khusus untuk shell expansion
  - CGI yang lemah sehingga dapat mengambil berkas yang seharusnya tidak berhak atau mengeksekusi perintah yang seharusnya tidak dilakukan (misal: `wget trojanhorse`, `eksekusi trojanhorse`). Contoh kelemahan *awstats*
  - Kelemahan ASP di sistem Windows
  - Guestbook abuse dengan informasi sampah (link ke pornografi atau sekedar info yang berulang)

Web & SQL

- Banyak aplikasi (transaksi) menggunakan basis web untuk mengakses database
- Juga dynamic web site
- Database diakses melalui SQL
- Sayangnya seringkali implementasi teledor
- SQL injection attack
  - Memasukkan perintah-perintah SQL yang nakal dengan akibat yang berbeda (server down, database berubah)
  - ***; drop table***, tanda petik ‘, UNION/OR
  - Tidak terdeteksi oleh firewall atau IDS karena pada level aplikasi

Keamanan Client WWW

- Berhubungan dengan masalah privacy
  - Cookies untuk tracking kemana saja browsing
  - Pengiriman informasi pribadi
- Attack (via active script, javascript, java)
  - Pengiriman data-data komputer (program apa yang terpasang, dsb.)
  - DoS attack (buka windows banyak)
  - Penyusupan virus, trojan horse, spyware
  - Security hole di JPEG bisa mengeksekusi aplikasi di sisi client

Penutup

- WWW merupakan salah satu aplikasi utama Internet dan Intranet
- Meskipun memiliki banyak keuntungan, sistem www masih banyak lubang keamanan – baik di sisi server maupun di sisi client