SECURE SOCKET LAYER (SSL)

Jaringan Komputer

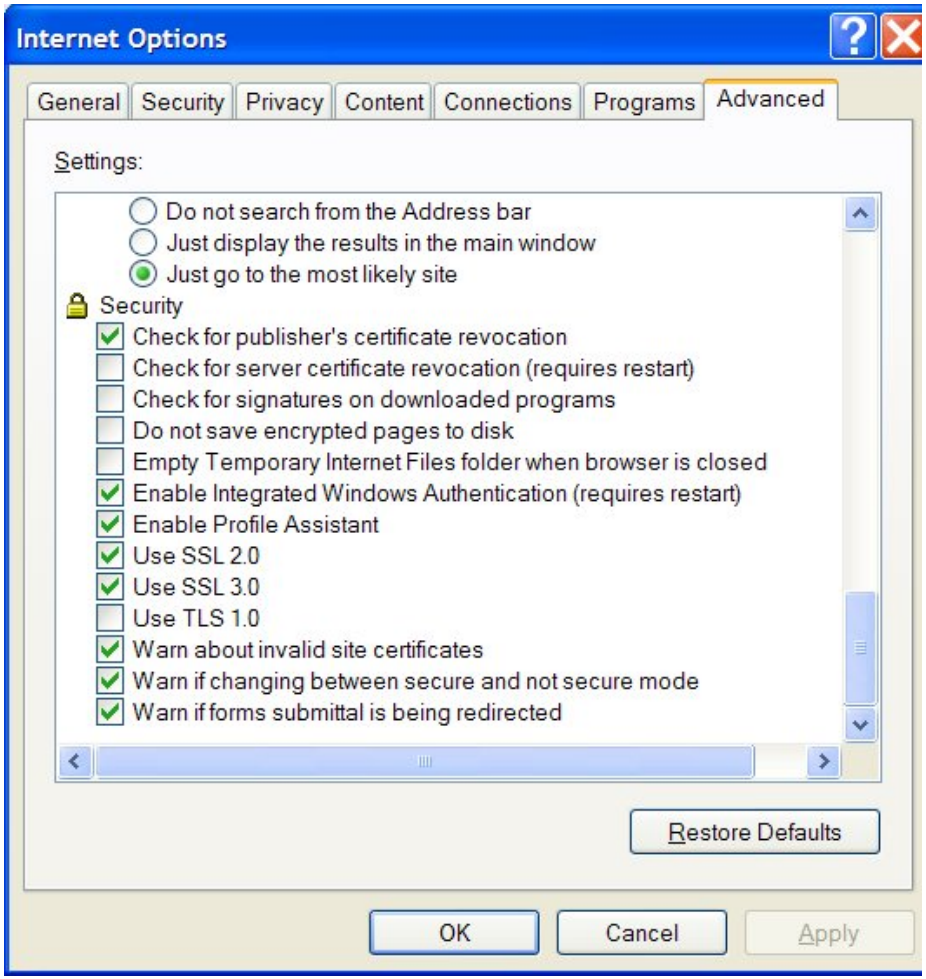
Keamanan Web

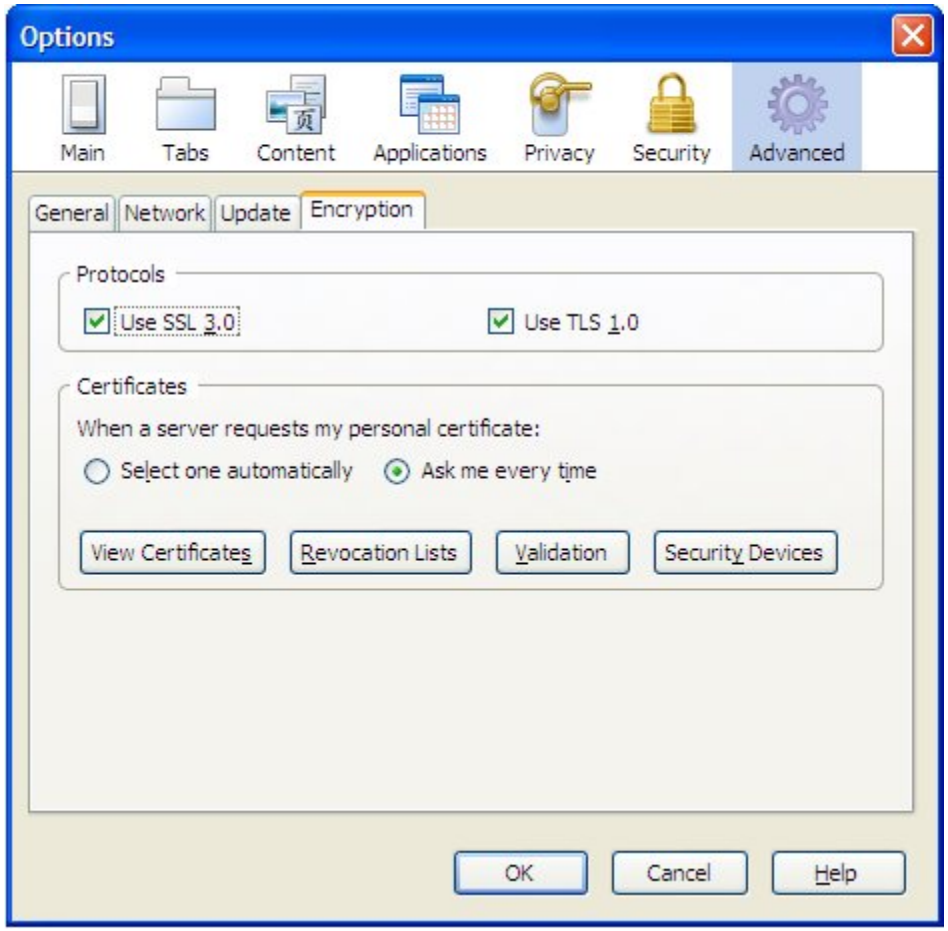
- *Secure Socket Layer* (*SSL*) adalah protokol yang digunakan untuk *browsing web* secara aman.
- *SSL* bertindak sebagai protokol yang mengamankan komunikasi antara *client* dan *server*.
- *SSL* dikembangkan oleh *Netscape Communications* pada tahun 1994.
- Ada beberapa versi *SSL*, versi 2 dan versi 3, tetapi versi 3 paling banyak digunakan saat ini.

- Untuk memastikan apakah *Internet Explorer* sudah siap menjalankan protokol *SSL*, klik dari *IE*:

  Tools → *Internet Options* → *Advanced*

  lalu cari pilihan *Security*, kemudian periksa apakah *SSL* versi 2.0 atau *SSL* versi 3.0 telah diberi tanda √ (Gambar 25.5).





TCP/IP

- *SSL* beroperasi antara protokol komunikasi *TCP/IP* (*Transmission Control Protocol/Internet Protocol*) dan aplikasi.
- *SSL* seolah-olah berlaku sebagai lapisan (*layer*) baru antara lapisan transport (*TCP*) dan lapisan aplikasi.
- *TCP/IP* adalah standard protokol yang digunakan untuk menghubungkan komputer dan jaringan dengan jaringan dari jaringan yang lebih besar, yaitu Internet.

Application (*HTTP*, *FTP*, *Telnet*)
Security (*SSL*)
Transport (*TCP*)
Network (*IP*)
Data link (*PPP*)
Phyiscal (*modem*, *ADSL*, *cable* TV)

Gambar 25.5 Lapisan (dan protokol) untuk *browsing* dengan *SSL*

Cara kerja TCP/IP (tanpa SSL)

- Kebanyakan transmisi pesan di Internet dikirim sebagai kumpulan potongan pesan yang disebut paket.
- *IP* bertanggung jawab untuk merutekan paket (lintasan yang dilalui oleh paket).
- Pada sisi penerima, *TCP* memastikan bahwa suatu paket sudah sampai, menyusunnya sesuai nomor urut, dan menentukan apakah paket tiba tanpa mengalami perubahan.
- Jika paket mengalami perubahan atau ada data yang hilang, *TCP* meminta pengiriman ulang.

- *TCP/IP* tidak memiliki pengamanan komunikasi yang bagus.
- *TCP/IP* tidak dapat mengetahui jika pesan diubah oleh pihak ketiga (*man-in-the-middle attack*).
- *SSL* membangun hubungan (*connection*) yang aman antara dua *socket*, sehingga pengiriman pesan antara dua entitas dapat dijamin keamanannya.

- Perlu dicatat bahwa *SSL* adalah protokol *client-server*, yang dalam hal ini *web browser* adalah *client* dan *website* adalah *server*.

- *Client* yang memulai komunikasi, sedangkan *server* memberi respon terhadap permintaan *client*.

- Protokol *SSL* tidak bekerja kalau tidak diaktifkan terlebih dahulu (biasanya dengan meng-klik tombol yang disediakan di dalam *web server*)

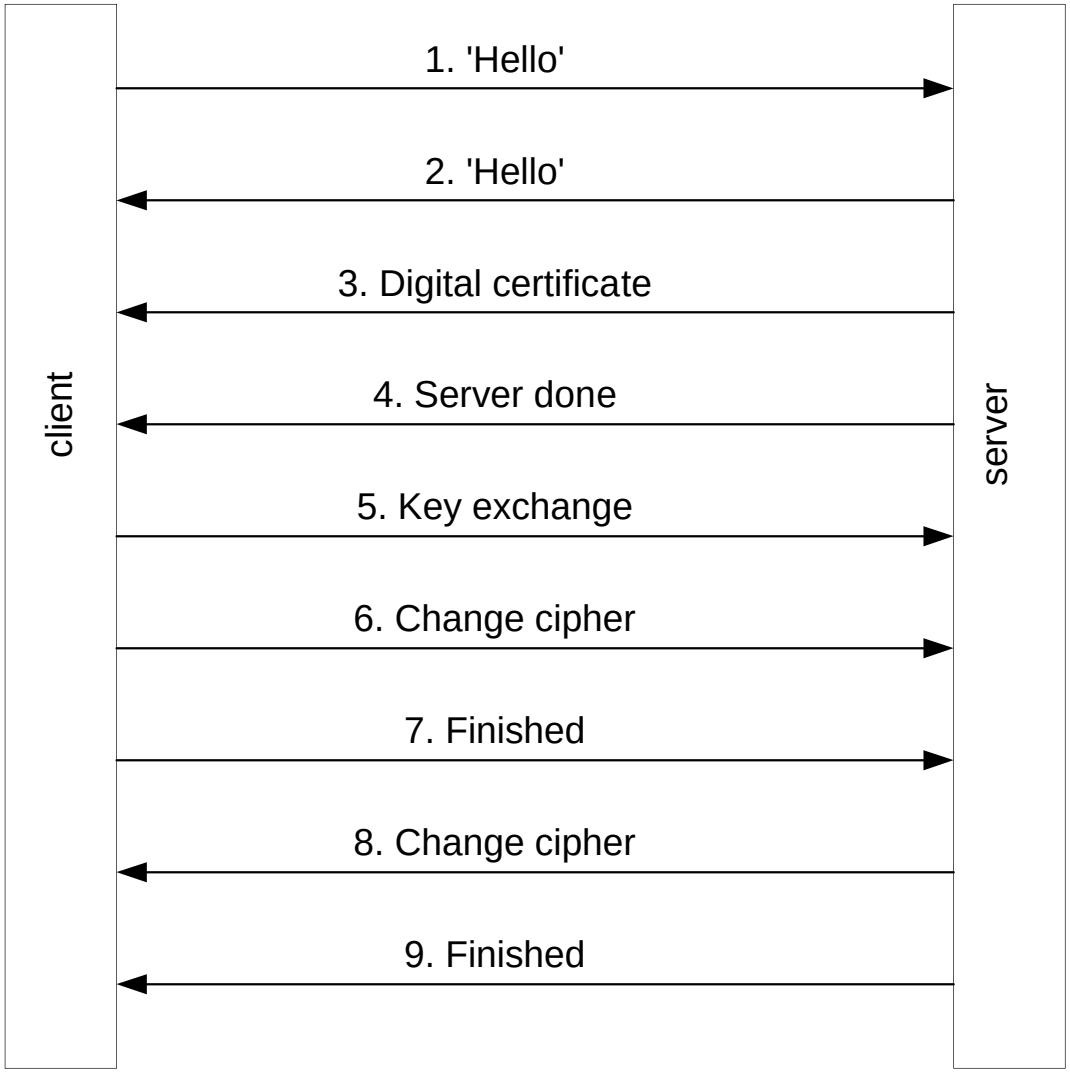
Komponen SSL

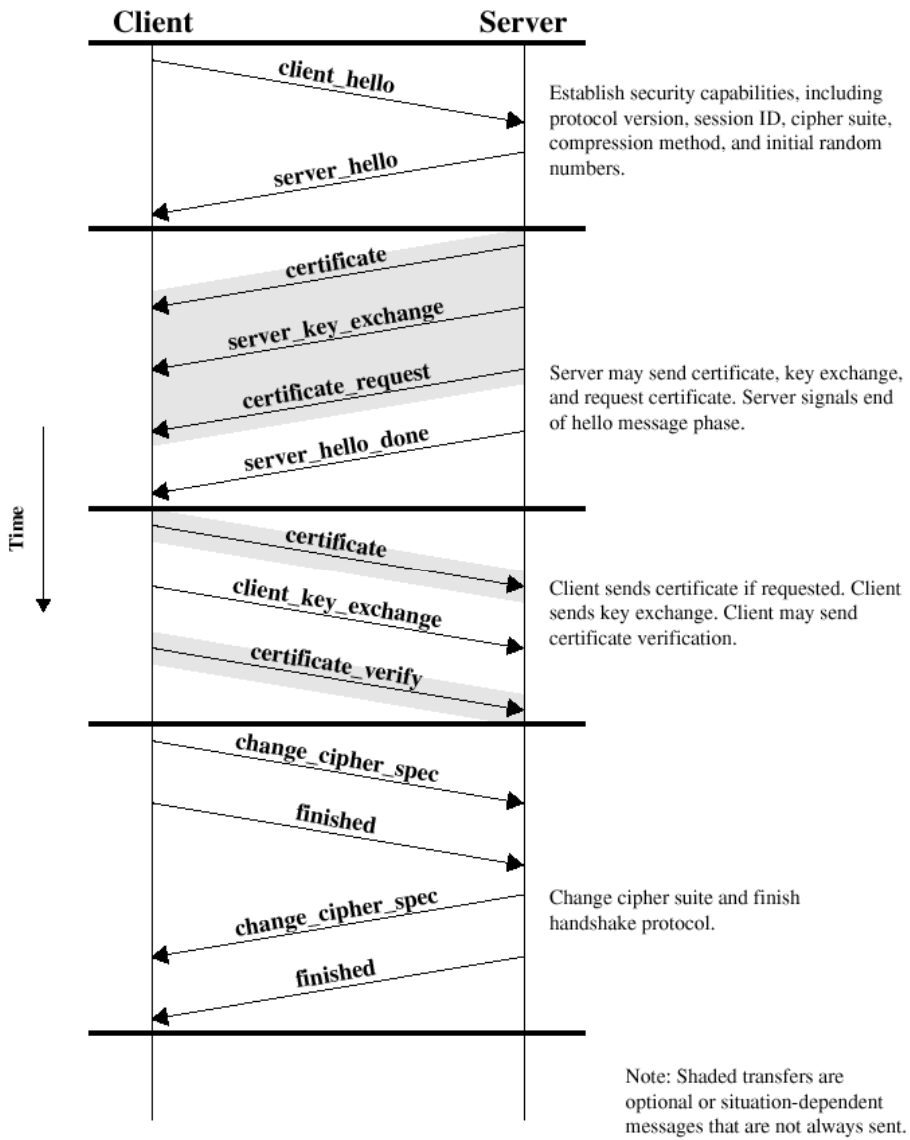
- SSL disusun oleh dua sub protokol:
  1. SSL handshaking, yaitu sub-protokol untuk membangun koneksi (kanal) yang aman untuk berkomunikasi.
  2. SSL record, yaitu sub-protokol yang menggunakan kanal yang sudah aman. SSL Record membungkus seluruh data yang dikirim selama koneksi.

Sub-protokol *handshaking*

- The most complex part of SSL.
- Allows the server and client to authenticate each other.
- Negotiate encryption, MAC algorithm and cryptographic keys.
- Used before any application data are transmitted.

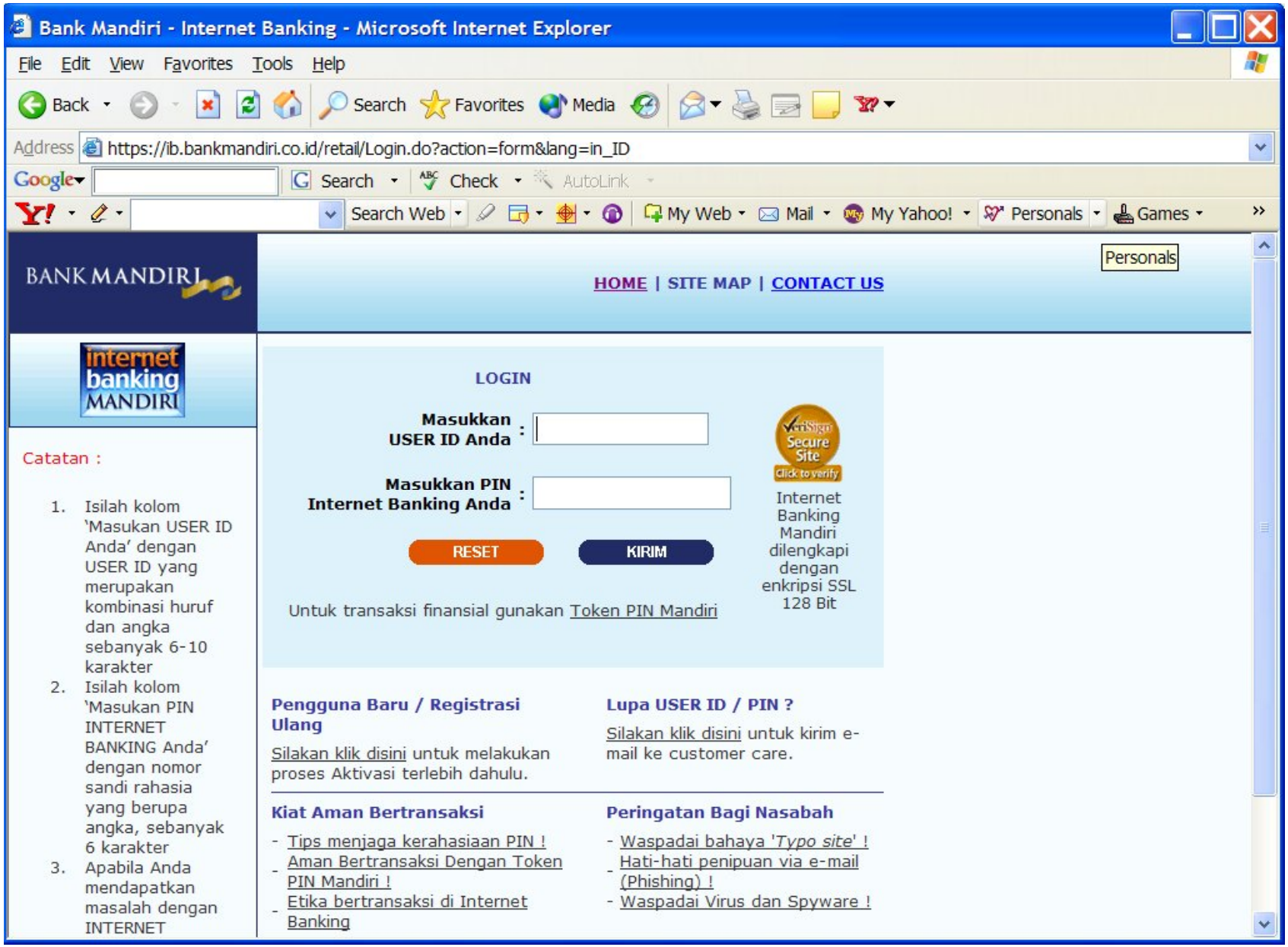
Sub-protokol *handshaking*




Client
Server
client_hello
server_hello
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time
certificate
client_key_exchange
certificate_verify
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
change_cipher_spec
finished
change_cipher_spec
finished
Change cipher suite and finish handshake protocol.
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

- Sampai di sini, proses pembentukan kanal yang aman sudah selesai.

- Bila sub-protokol ini sudah terbentuk, maka *http://* pada *URL* berubah menjadi *https://* (*http secure*)


Bank Mandiri - Internet Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://ib.bankmandiri.co.id/retail/Login.do?action=form&lang=in_ID
Google Search Check AutoLink
Search Web My Web Mail My Yahoo! Personals Games
BANK MANDIRI
Personals
HOME | SITE MAP | CONTACT US
internet banking MANDIRI
Catatan :
1. Isilah kolom 'Masukan USER ID Anda' dengan USER ID yang merupakan kombinasi huruf dan angka sebanyak 6-10 karakter
2. Isilah kolom 'Masukan PIN INTERNET BANKING Anda' dengan nomor sandi rahasia yang berupa angka, sebanyak 6 karakter
3. Apabila Anda mendapatkan masalah dengan INTERNET
LOGIN
Masukkan USER ID Anda :
Masukkan PIN Internet Banking Anda :
RESET
KIRIM
Untuk transaksi finansial gunakan Token PIN Mandiri
VeriSign Secure Site Click to verify
Internet Banking Mandiri dilengkapi dengan enkripsi SSL 128 Bit
Pengguna Baru / Registrasi Ulang
Silakan klik disini untuk melakukan proses Aktivasi terlebih dahulu.
Lupa USER ID / PIN ?
Silakan klik disini untuk kirim e-mail ke customer care.
Kiat Aman Bertransaksi
- Tips menjaga kerahasiaan PIN !
- Aman Bertransaksi Dengan Token PIN Mandiri !
- Etika bertransaksi di Internet Banking
Peringatan Bagi Nasabah
- Waspadai bahaya 'Typo site' !
- Hati-hati penipuan via e-mail (Phishing) !
- Waspadai Virus dan Spyware !