

II4031 Kriptografi dan Koding



Secure Socket Layer (SSL)

Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
ITB

Protokol Kriptografi

- Protokol: aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan.
- Protokol kriptografi: protokol yang menggunakan kriptografi. Orang yang berpartisipasi dalam protokol kriptografi memerlukan protokol tersebut misalnya untuk:
 - berbagi komponen rahasia untuk menghitung sebuah nilai,
 - membangkitkan rangkaian bilangan acak,
 - meyakinkan identitas orang lainnya (otentikasi),
 - mengenkripsi dan dekripsi pesan
 - dll



- Protokol kriptografi dibangun dengan melibatkan beberapa algoritma kriptografi.
- Sebagian besar protokol kriptografi dirancang untuk dipakai oleh kelompok yang terdiri dari 2 orang pemakai.
- Tetapi ada juga beberapa protokol yang dirancang untuk dipakai oleh kelompok yang terdiri dari lebih dari dua orang pemakai (misalnya pada aplikasi *teleconferencing*)



Contoh-contoh Protokol Kriptografi

1. **Secure Socket Layer (SSL)**
2. IPSec (Internet Protocol Security)
3. Kerberos
4. Protokol pertukaran kunci Diffie-Hellman
5. Transport Layer Security (TLS)



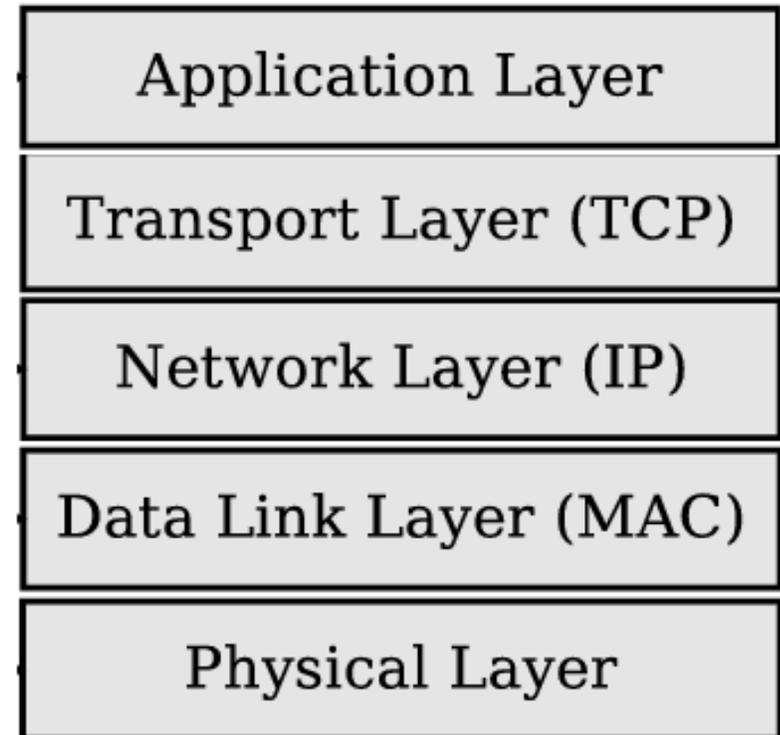
Keamanan Web

- *Secure Socket Layer (SSL)* adalah protokol kriptografi 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.

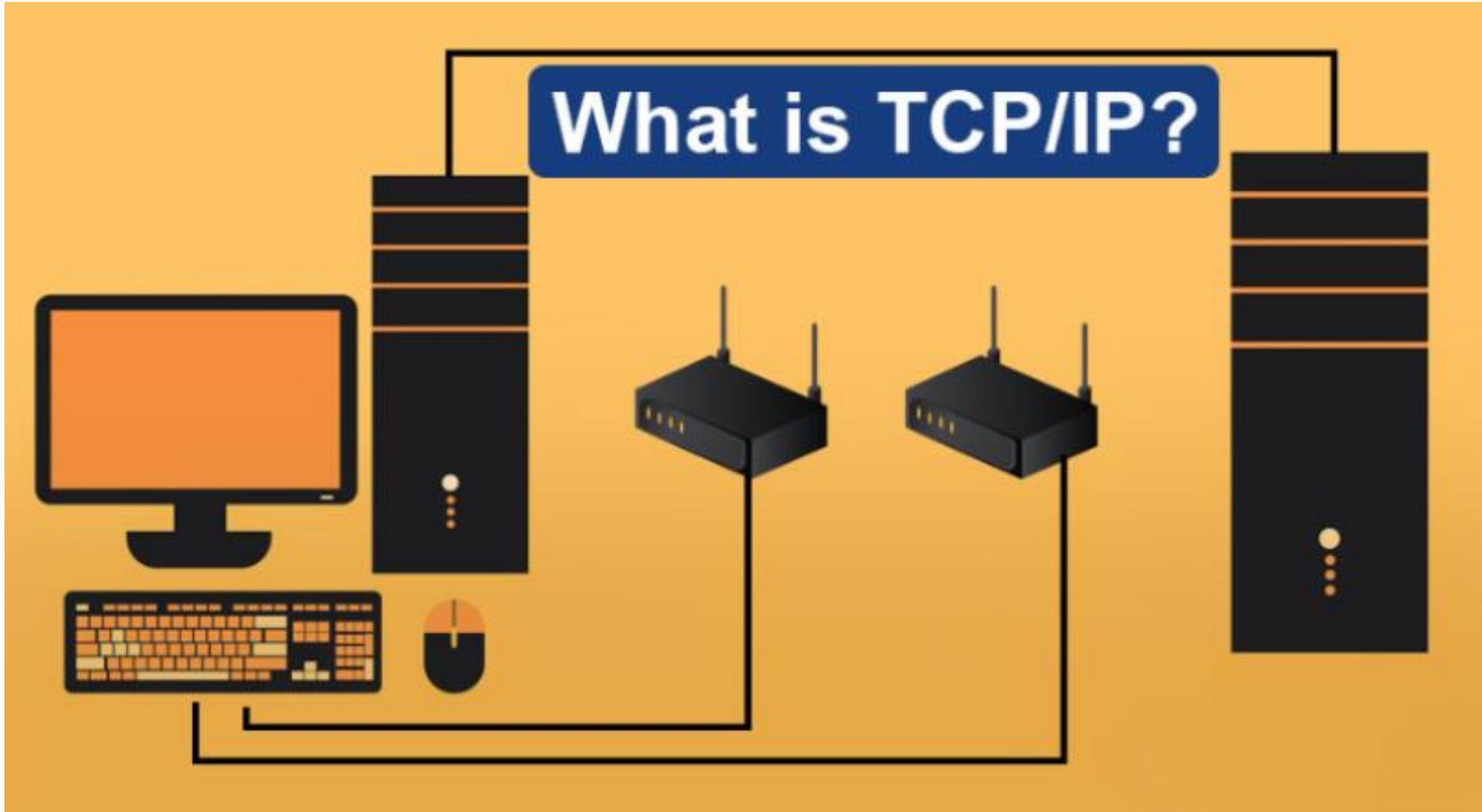
TCP/IP

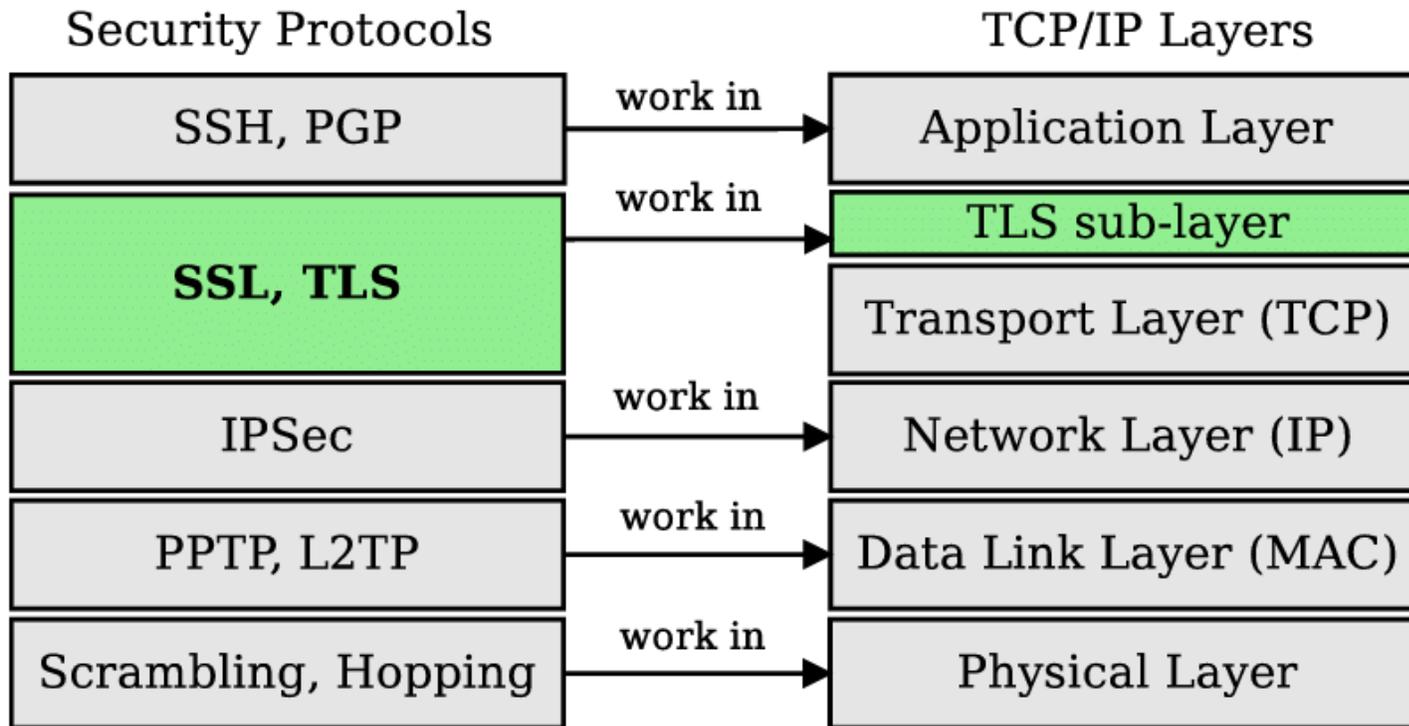
- *TCP/IP* adalah standard protokol yang digunakan untuk menghubungkan komputer dan jaringan dengan jaringan yang lebih besar, yaitu Internet.

TCP/IP Layers



What is 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 transpor (*TCP*) dan lapisan aplikasi.

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-protocol (*layer*):

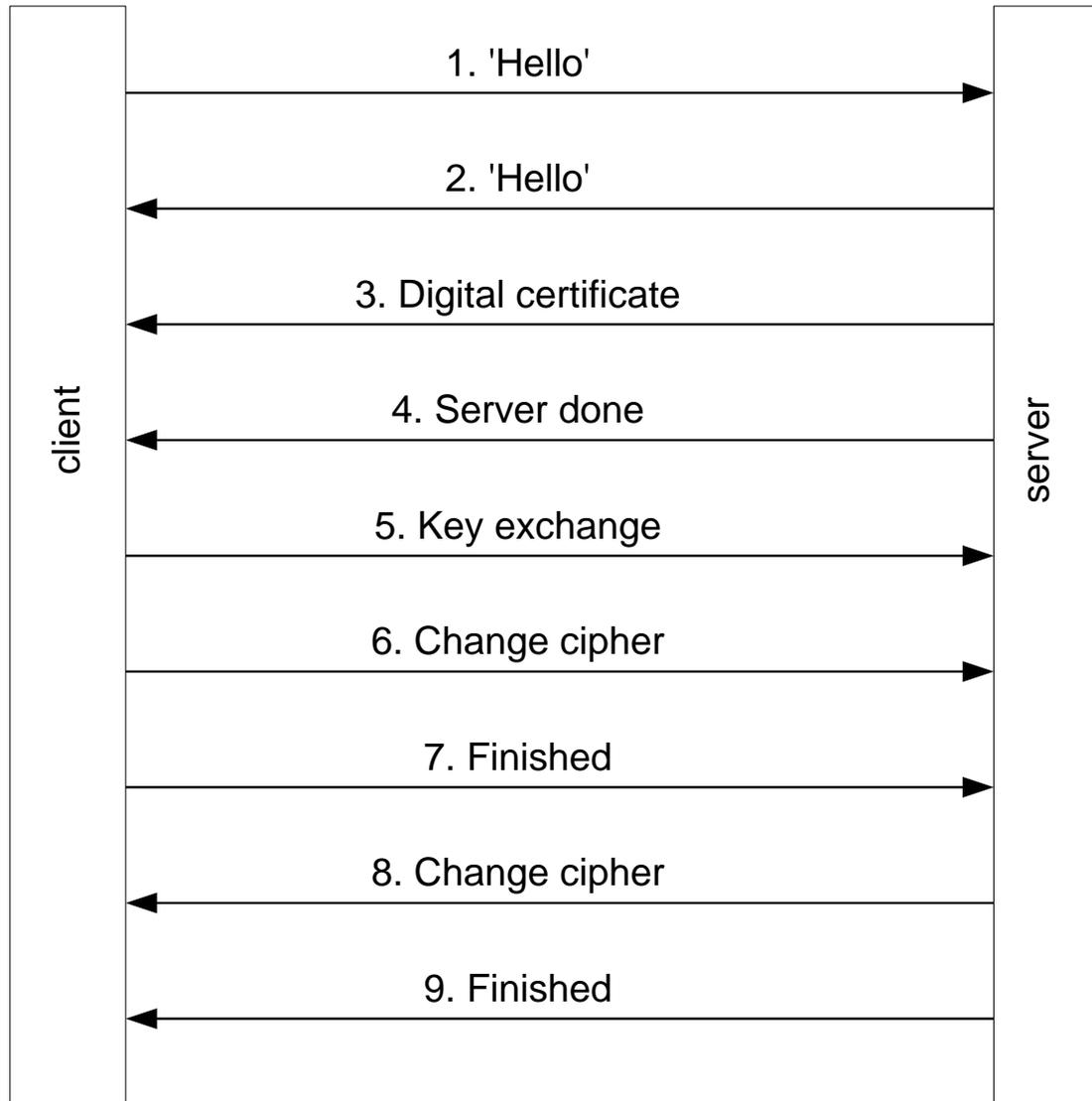
1. *SSL handshaking*, yaitu sub-protokol untuk membangun koneksi (kanal) yang aman untuk berkomunikasi,
2. *SSL record*, yaitu sub-protokol yang menggunakan kanal yang sudah aman. *SSL Record* membungkus seluruh data yang dikirim selama koneksi.

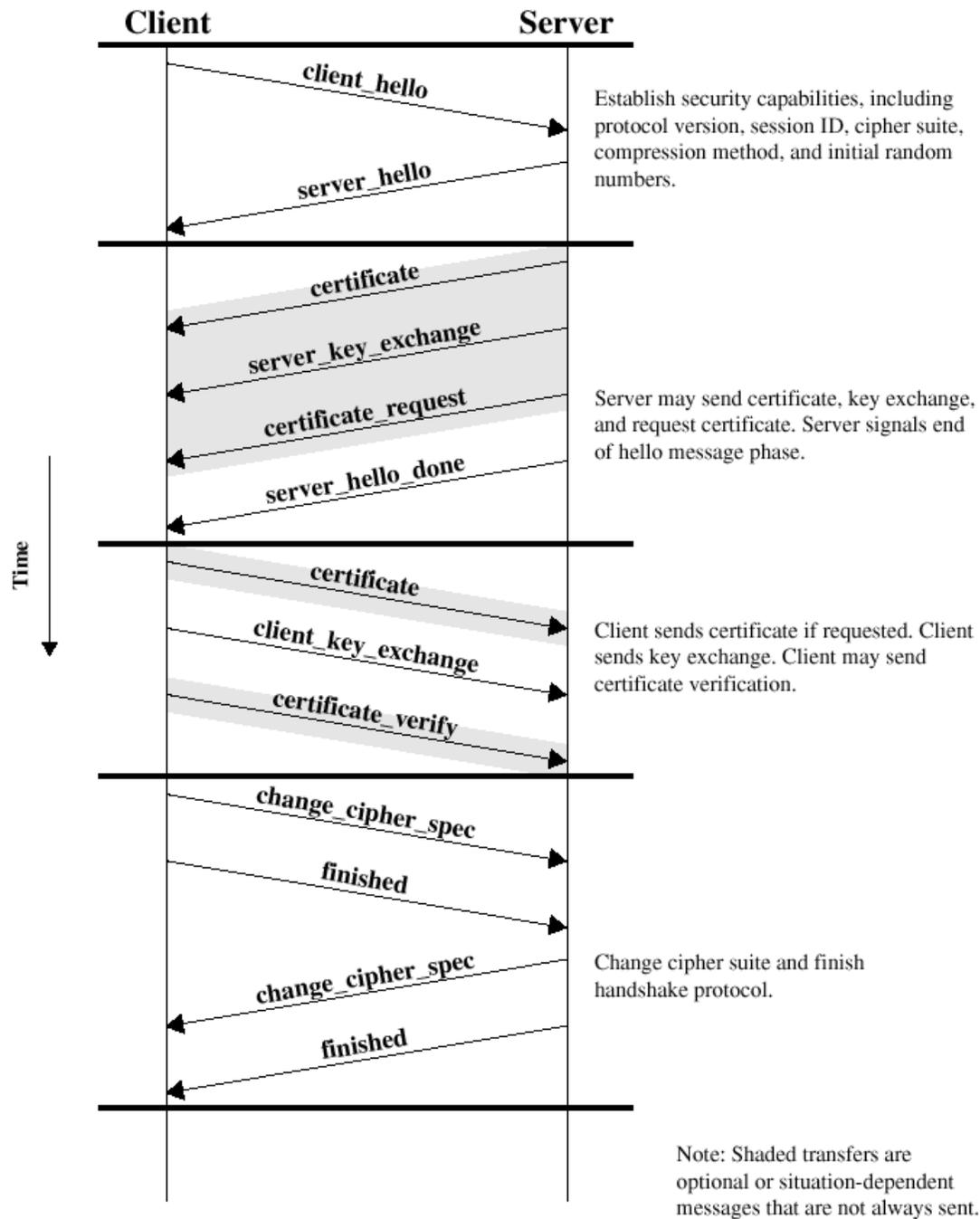
Sub-protokol *handshaking*

- 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.

Sumber: William Stalling

Sub-protokol *handshaking*





- 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 Forward Stop Refresh Home 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 HOME | SITE MAP | CONTACT US Personals

internet banking MANDIRI

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

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

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.

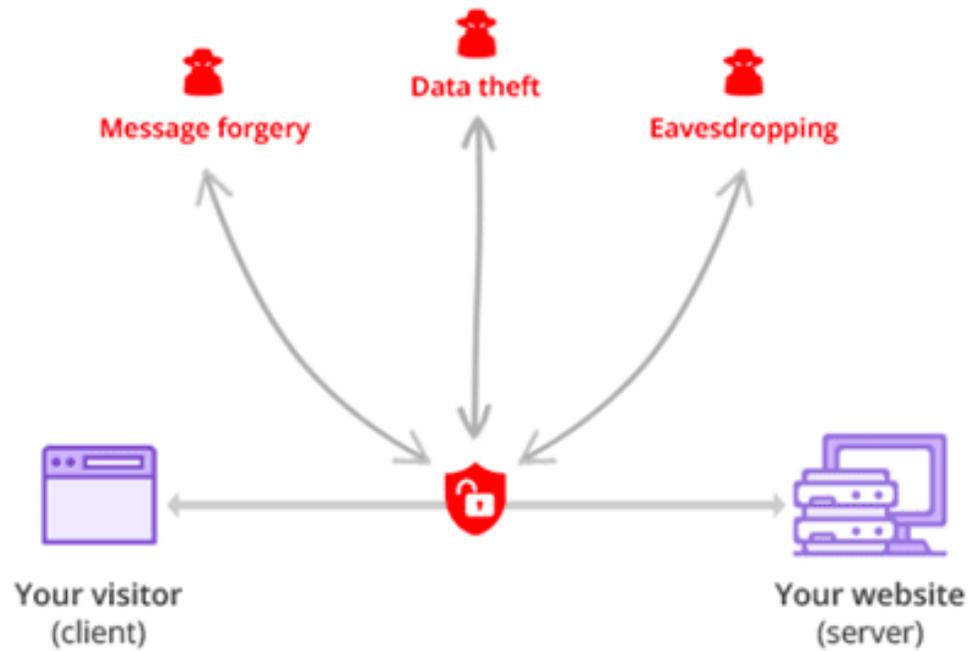
Kiat Aman Bertransaksi

- [Tips menjaga kerahasiaan PIN ! Aman Bertransaksi Dengan Token PIN Mandiri !](#)
- [Etika bertransaksi di Internet Banking](#)

Peringatan Bagi Nasabah

- [Waspada bahaya 'Typo site' !](#)
- [Hati-hati penipuan via e-mail \(Phishing\) !](#)
- [Waspada Virus dan Spyware !](#)

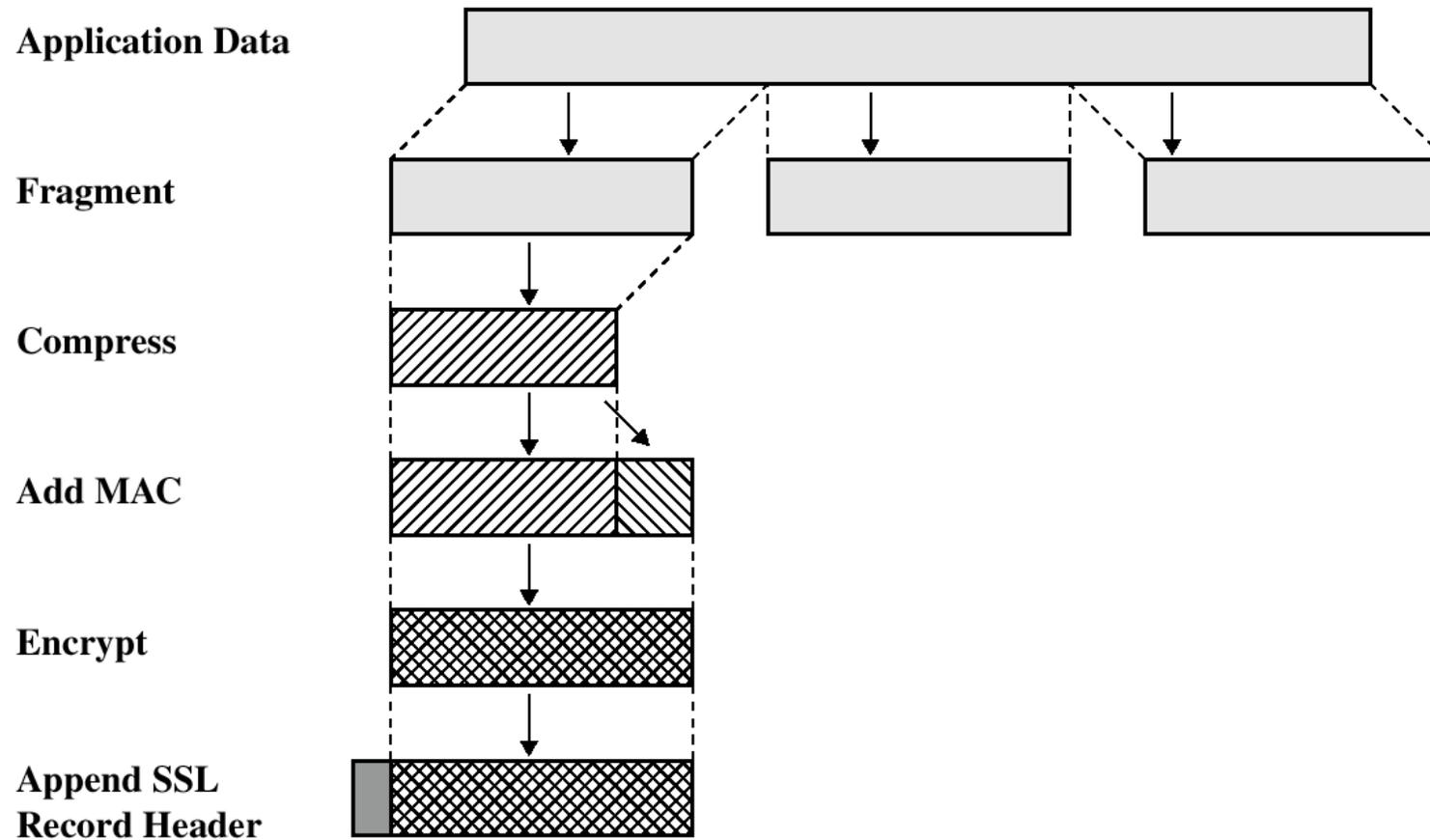
HTTP: No Encryption (no SSL)



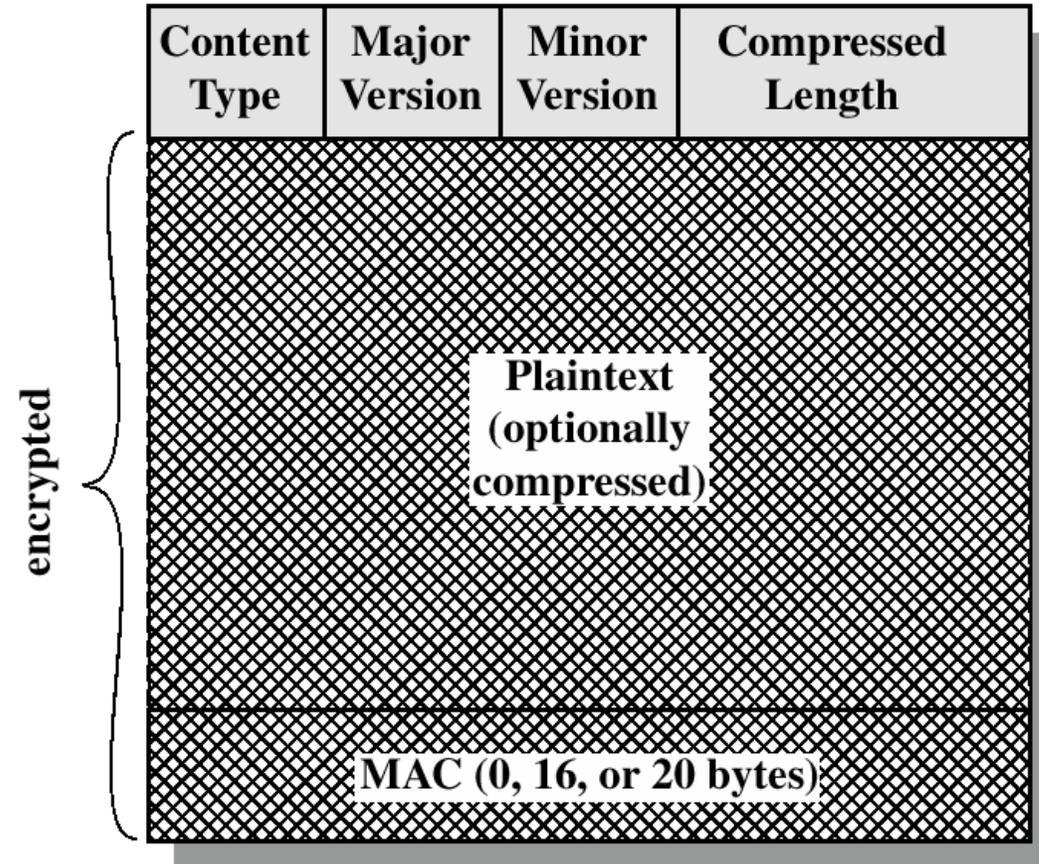
HTTPS: Secure Cheap SSL Connection



Sub-protokol *SSL record*



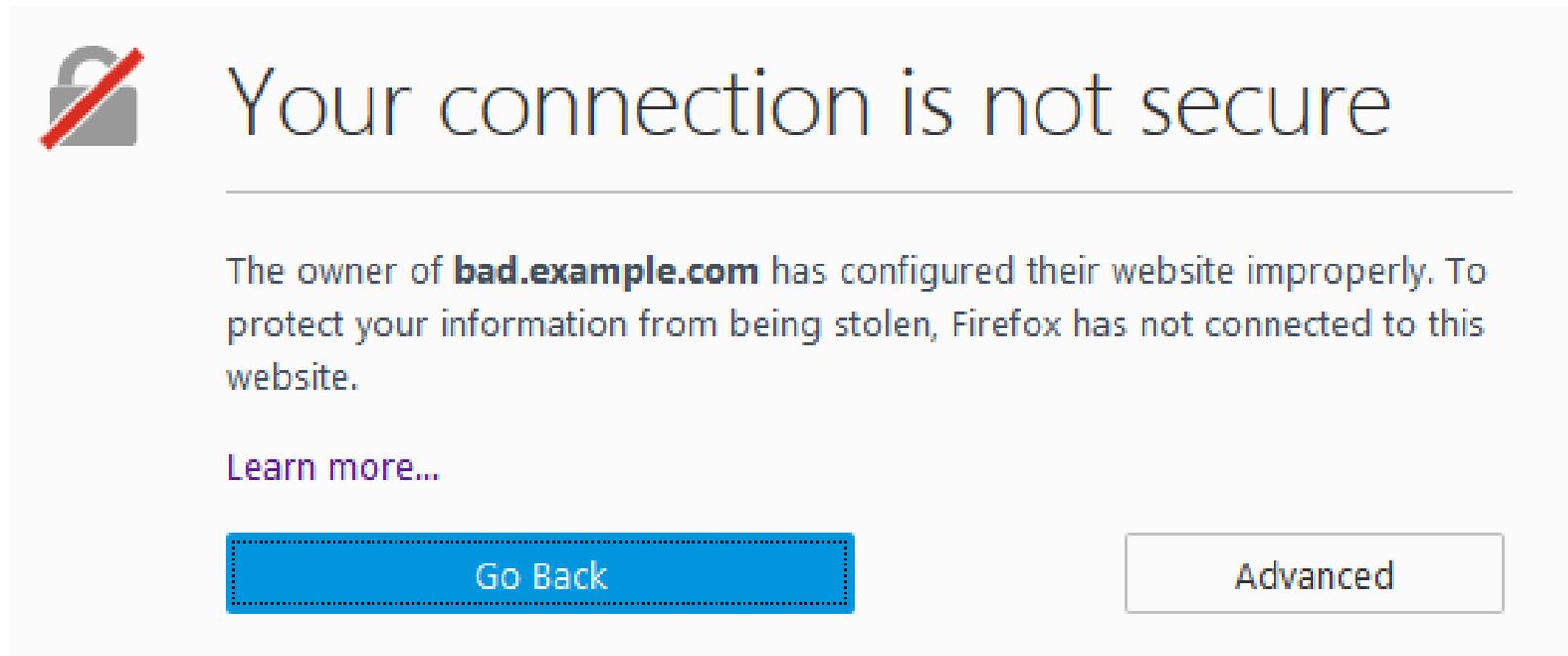
SSL Record Format



- Di tempat penerima, sub-protokol *SSL Record* melakukan proses berkebalikan: mendekripsi data yang diterima, mengotentikasinya (dengan *MAC*), men-dekompresinya, lalu merakitnya.
- Protokol SSL membuat komunikasi menjadi lebih lambat.
- Piranti keras, seperti kartu *peripheral component interconnect (PCI)* dapat dipasang ke dalam *web server* untuk memproses transaksi *SSL* lebih cepat sehingga mengurangi waktu pemrosesan
- Informasi lebih lanjut mengenai *SSL* dapat diperoleh dari tutorial *SSL* di www.netscape.com/security/index.html.

Sertifikat SSL

- Pernahkah mendapat pesan seperti ini dari *browser* atau *google* ketika mengunjungi sebuah website:



- Itu artinya *website* tersebut tidak menggunakan [sertifikat SSL](#) dan transmisi data yang terjadi tidak akan aman.

TLS (Transport Layer Security)

- Pada Tahun 1996, *Netscape Communications Corp.* mengajukan *SSL* ke *IETF (Internet Engineering Task Force)* untuk standarisasi.
- Hasilnya adalah *TLS (Transport Layer Security)*. *TLS* dijelaskan di dalam *RFC 2246*
- Untuk informasi lebih lanjut perihal *TLS*, kunjungi situs *IETF* di www.ietf.org/rfc/rfc2246.
- *TLS* dapat dianggap sebagai *SSL* versi 3.1, dan implementasi pertamanya adalah pada Tahun 1999

Transport Layer Security (TLS)

- The same record format as the SSL record format.
- Defined in RFC 2246.
- Similar to SSL v3.
- Differences in the:
 - version number
 - message authentication code
 - pseudorandom function
 - alert codes
 - cipher suites
 - client certificate types
 - certificate_verify and finished message
 - cryptographic computations
 - padding