Secure Socket Layer (SSL)

DITISS 2015

SSL (Secure Sockets Layer)

- Developed by Netscape
- Provides a secure channel between communicating devices on the net
- SSL is a protocol in the network protocol stack. It resides between the application and the TCP/IP protocols (illustrated in the next slide)
- In theory SSL can be used by any application level protocol but at the moment it is used for securing HTTP transactions

SSL (Secure Sockets Layer)

- By far, the dominant security technology on the web is SSL
- Transport Layer Security
  - HTTPS is HTTP over SSL
- Responsible for the emergence of e-commerce, other security sensitive services on the web
- Beneficiary of several years of public scrutiny

What is provided by SSL

- Confidentiality (privacy)
- Data Integrity (Tamper Proofing)
- Server Authentication (Proving a server is what it claims it is)
- Used in typical B2C transaction
- Optional Client Authentication would be required in B2B (or web services environment in which program talks to program)

SSL …

<table>
<tr><td>SSL Handshake Protocol</td><td>SSL Change Cipher Spec Protocol</td><td>SSL Alert protocol</td><td>HTTP</td></tr>
<tr><td colspan="4">SSL Record protocol</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

SSL protocol stack

SSL

- SSL Server Authentication
  - SSL-enabled client can use PKC to check that the server’s certificate and public ID are valid, and that the CA is trusted
- SSL Client Authentication
  - SSL-enabled server can check that a client’s certificate and public ID are valid, and that the CA is trusted
- Secure connection – client/server transmissions are encrypted, plus tamper detection

SSL

SSL exchanges messages that permit:

- client to authenticate the server (always)
- server to authenticate the client (optional)
- client and server negotiation of crypto algorithms that they both support
- using PKC to encrypt and exchange shared secrets
- establishing an encrypted SSL connection

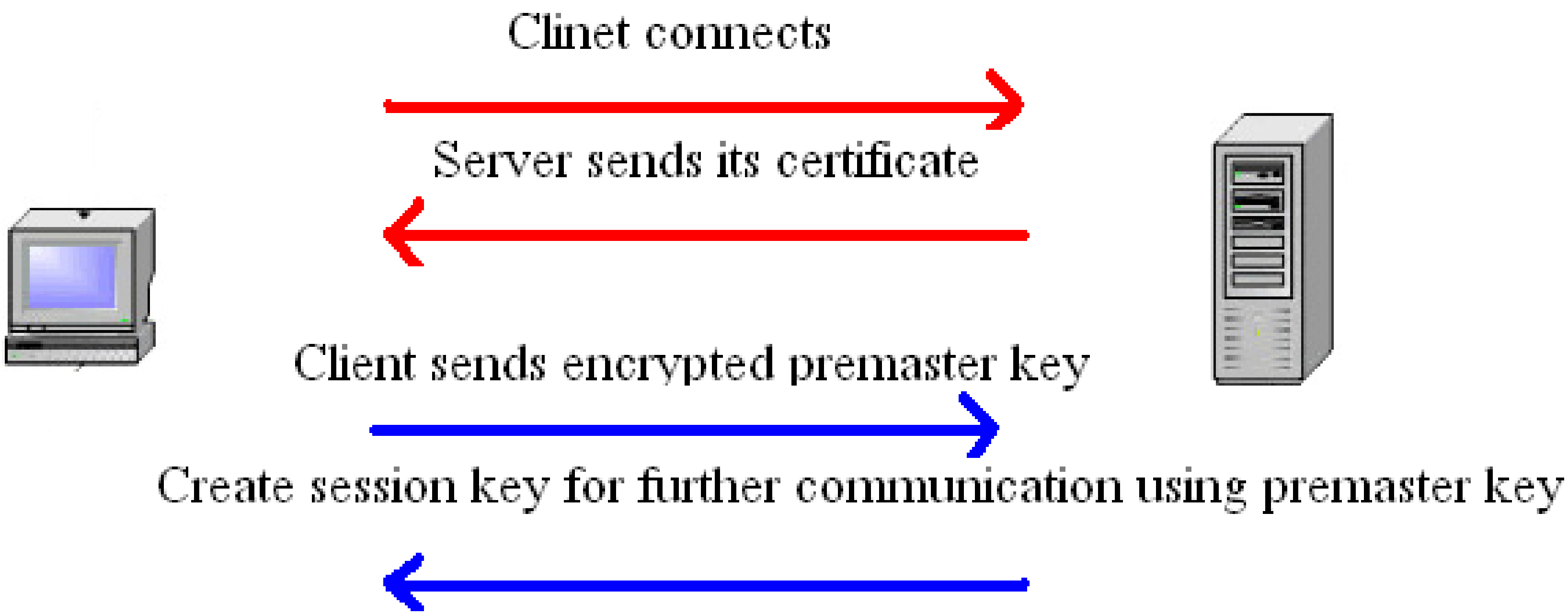
SSL and Security Keys

-Uses public/private key (asymmetric)
-Scheme to create secret key (symmetric)

-Secret key is then used for encryption of data
-SSL operation is optimized for performance:

-Using symmetric key for encryption is a lot faster than using asymmetric keys

SSL Key Exchange



Clinet connects

Server sends its certificate

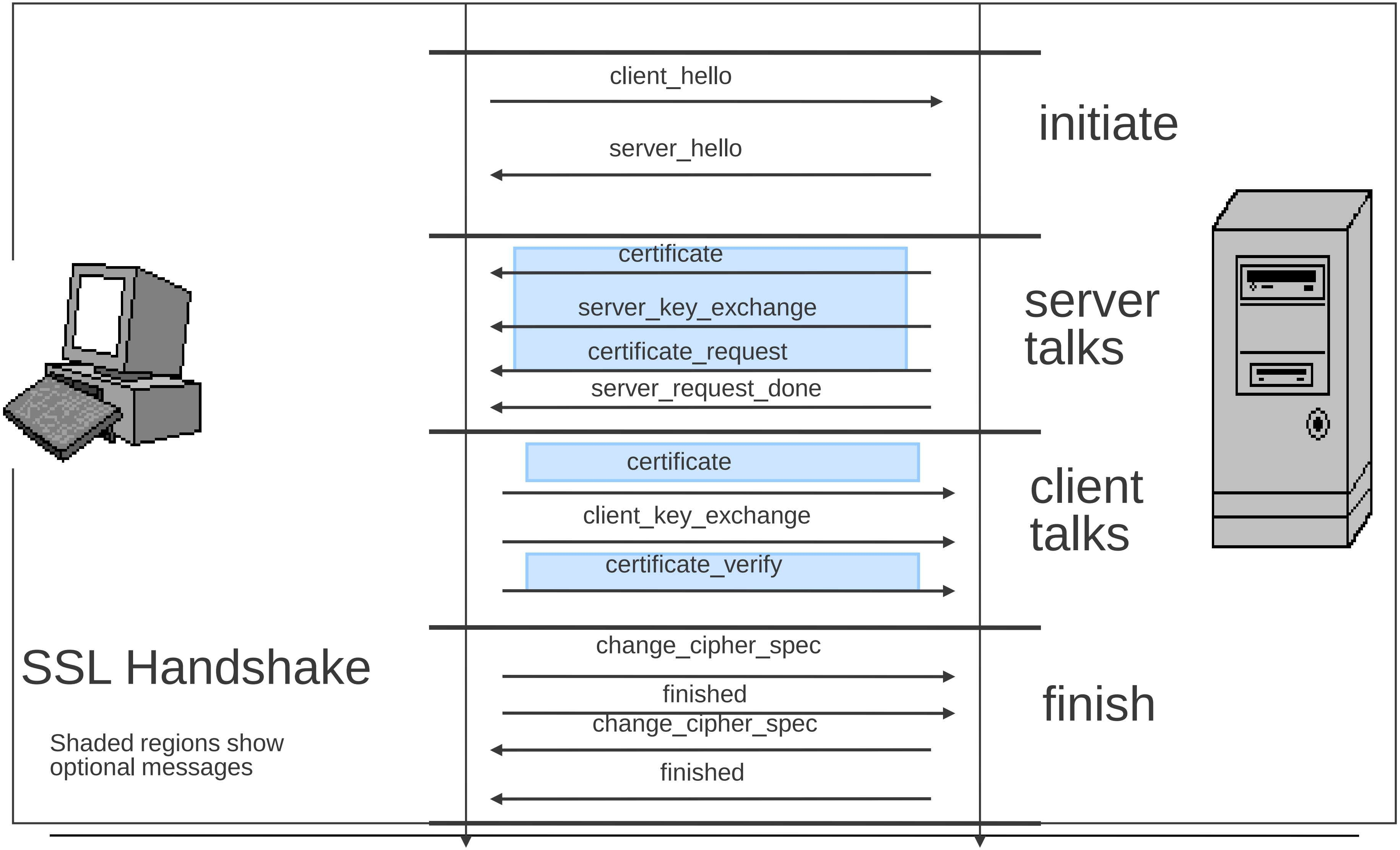
Client sends encrypted premaster key

Create session key for further communication using premaster key

SSL …

- The handshake protocol is used to set up the session.
- The record protocol is used to receive/transmit the data passed to it from the other sub-protocols (including the handshake protocol)
- The alert protocol is used to notify the peer entity of SSL related alerts
- The change cipher spec protocol is used for changing the the cipher spec.

SSL handshake protocol



initiate

client_hello

server_hello

server talks

certificate

server_key_exchange

certificate_request

server_request_done

client talks

certificate

client_key_exchange

certificate_verify

finish

change_cipher_spec

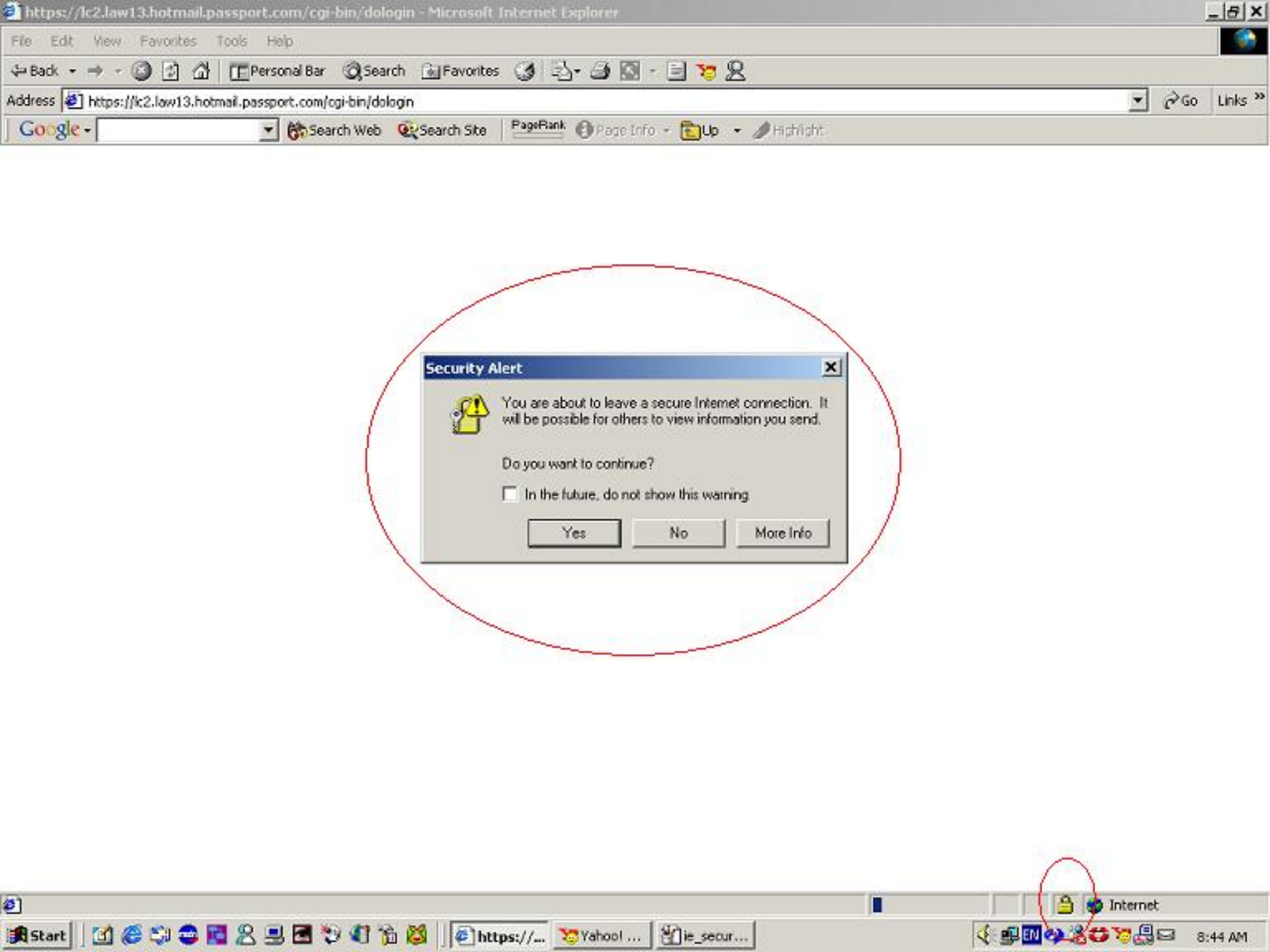
finished

change_cipher_spec

finished

SSL Handshake

Shaded regions show
optional messages



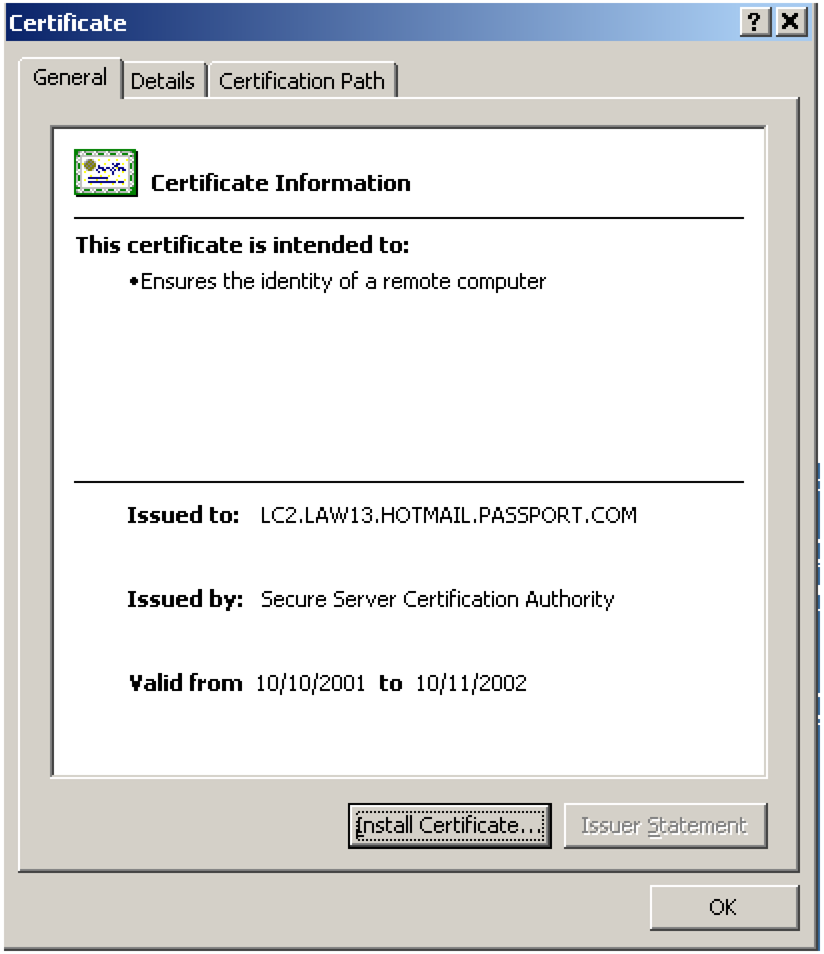
https://lc2.law13.hotmail.passport.com/cgi-bin/dologin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Personal Bar
Search
Favorites
Address
https://lc2.law13.hotmail.passport.com/cgi-bin/dologin
Go
Links
Google
Search Web
Search Site
PageRank
Page Info
Up
Highlight
Yes
No
More Info
Internet
Start
https://...
Yahoo! ...
ie_secur...
EN
8:44 AM

Security Alert

You are about to leave a secure Internet connection. It will be possible for others to view information you send.

Do you want to continue?

□ In the future, do not show this warning



Certificate Information

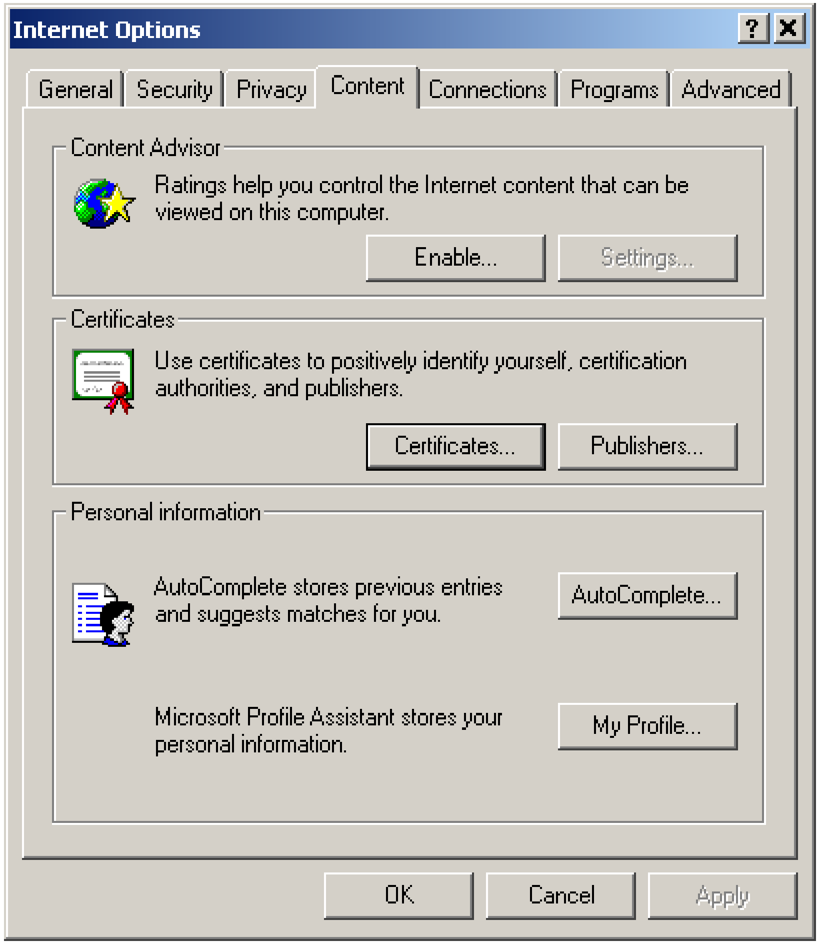
This certificate is intended to:

- Ensures the identity of a remote computer

Issued to: LC2.LAW13.HOTMAIL.PASSPORT.COM

Issued by: Secure Server Certification Authority

Valid from 10/10/2001 **to** 10/11/2002



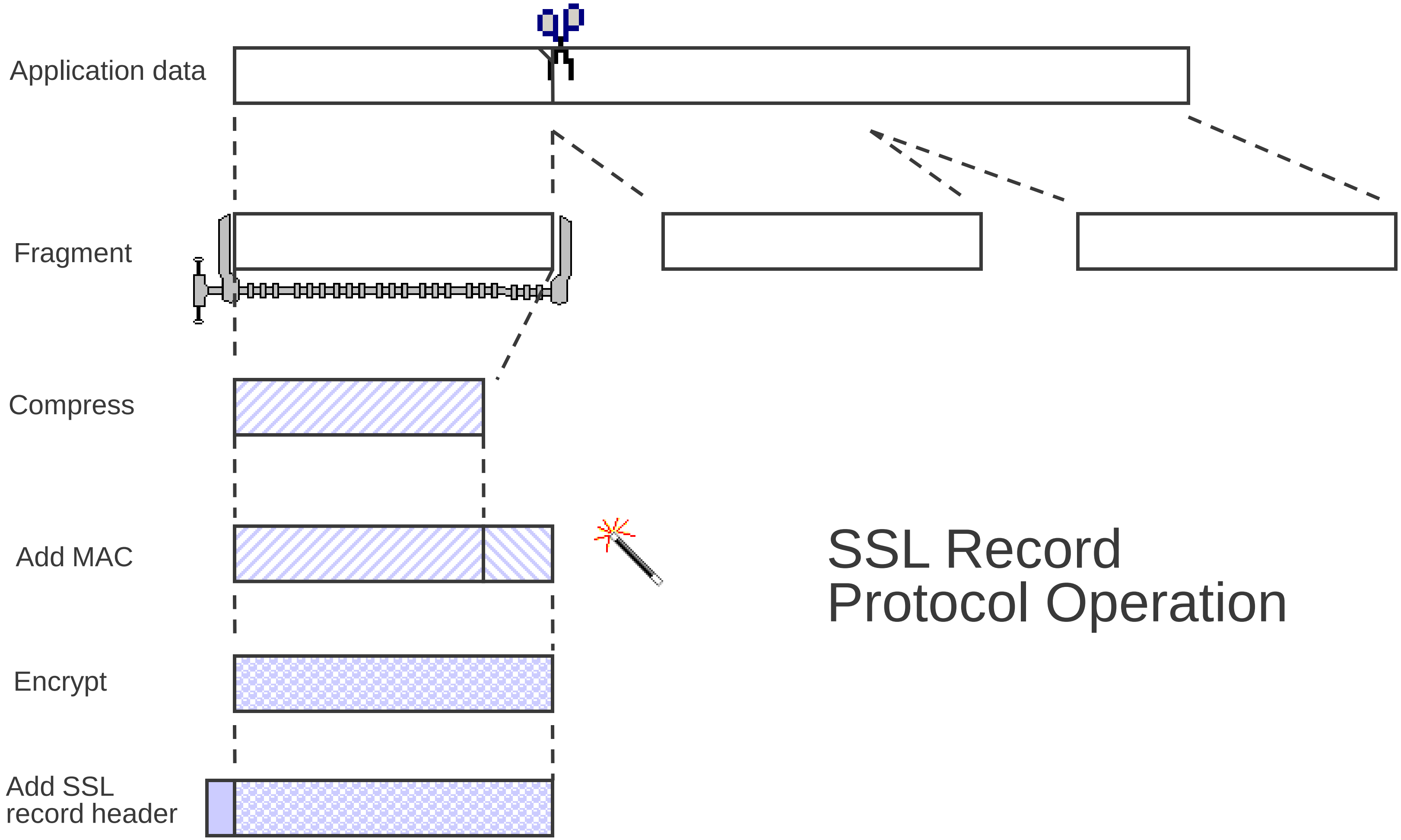
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

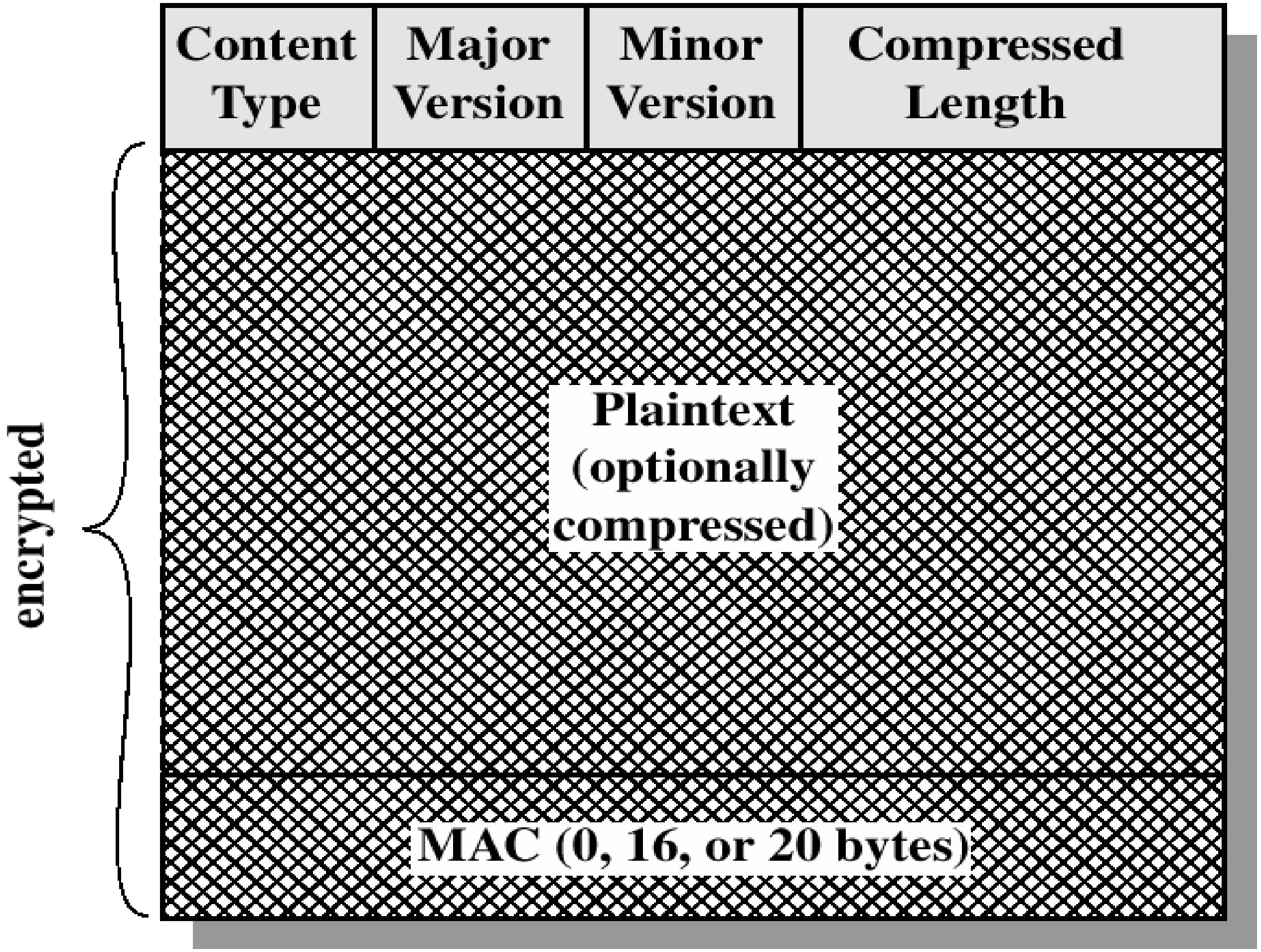
Microsoft Profile Assistant stores your personal information.

SSL Record protocol



SSL Record Protocol Operation

SSL Record Format



SSL Authentication

1. For server authentication, the client encrypts the premaster secret with the server's public key.

2. Only the server's private key could have decrypted that data.

3. For client authentication, client encrypts some data known to client and server with
client's private key (i.e., creates a digital signature).
Public key in client's certificate will validate the digital signature only if it was encrypted with the client's private key.

Server Authentication

Server's Certificate

Server's public key

Certificate's validity

Server's domain name

Issuer's domain name

Issuer's digital signature

1. Is today's date within validity period?

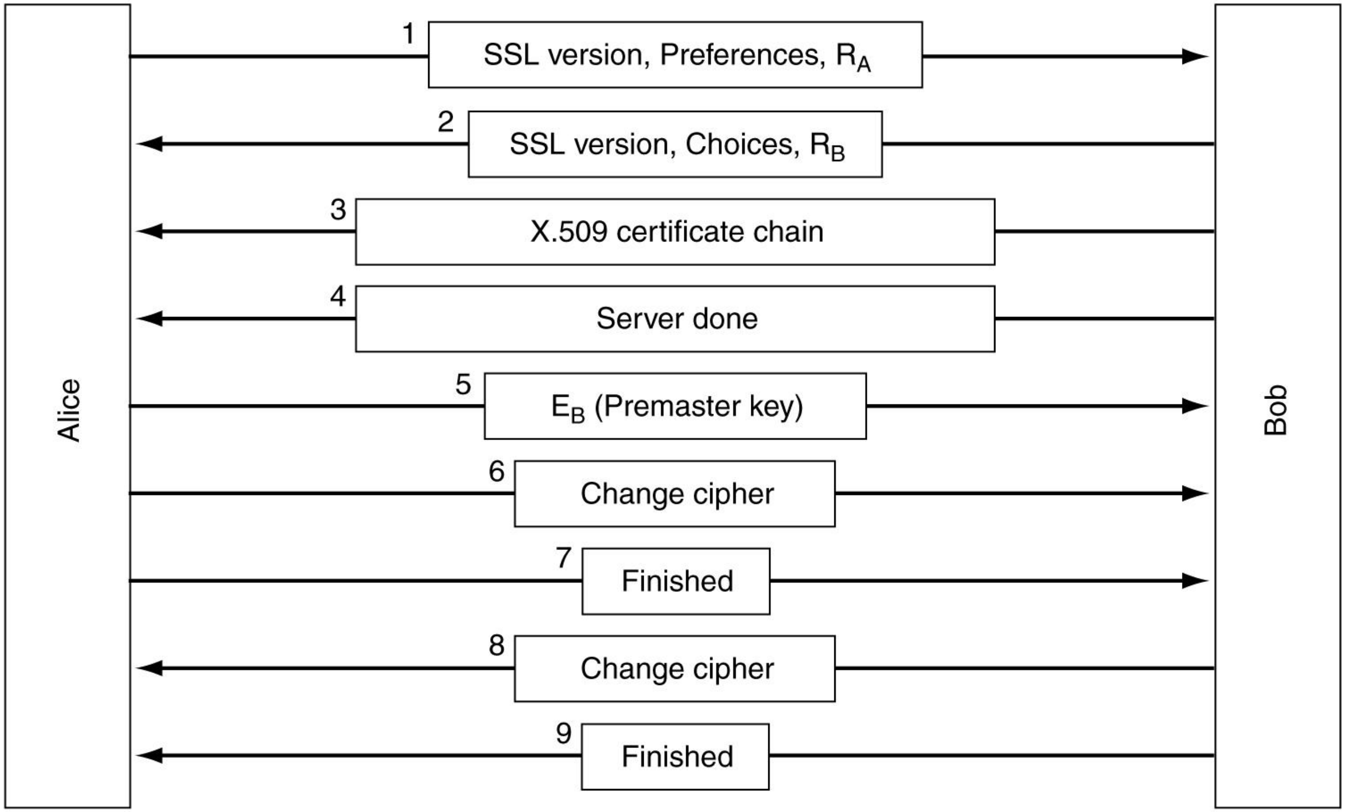
2. Is issuing CA a trusted CA?

3. Does issuing CA's public key validate the issuer's digital signature?

4. Does the domain name in the server's certificate match the domain name of the server itself?

SSL

- A simplified version of the SSL connection establishment sub-protocol.



References

- www.freeswan.org
- www.netbsd.org
- http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec_wp.htm
- www.rommel.stw.uni-erlangen.de/~hshoexer/ ipsec-howto/HOWTO.html
- support.microsoft.com/support/ kb/articles/q252/7/35.asp
- online.securityfocus.com/infocus/1519 - 37k
- www.labmice.net/networking/IPsec.htm

References

- Cryptography and Network security – principles and practice : William Stallings
- Applied Cryptography, Second Edition: Bruce Schneier
- www.certicom.com/index.php/ecc-turorial
- http://campustechnology.com/articles/39190_2
- http://csrc.nist.gov/
- Handbook of Applied Cryptography, by Menezes
- http://en.wikipedia.org
- Cryptographic Techniques for N/w Security

References…

- Cryptography & Network Security by William Stallings
- Applied Cryptography by Bruce Schnieir
- Lecture notes of various courses available online.
- http://www.oucs.ox.ac.uk/email/secure.html
- http://www.pgpi.org/
- http://www.pgpi.org/doc/faq/
- http://users.ox.ac.uk/~aesb/pgp.ppt

Thank You