Cryptography Application TLS / SSL

SANOG 27

25th January 2016 – 1st February 2016

Kathmandu, Nepal

Issue Date: [31-12-2015]

Revision: [V.1]

APNIC

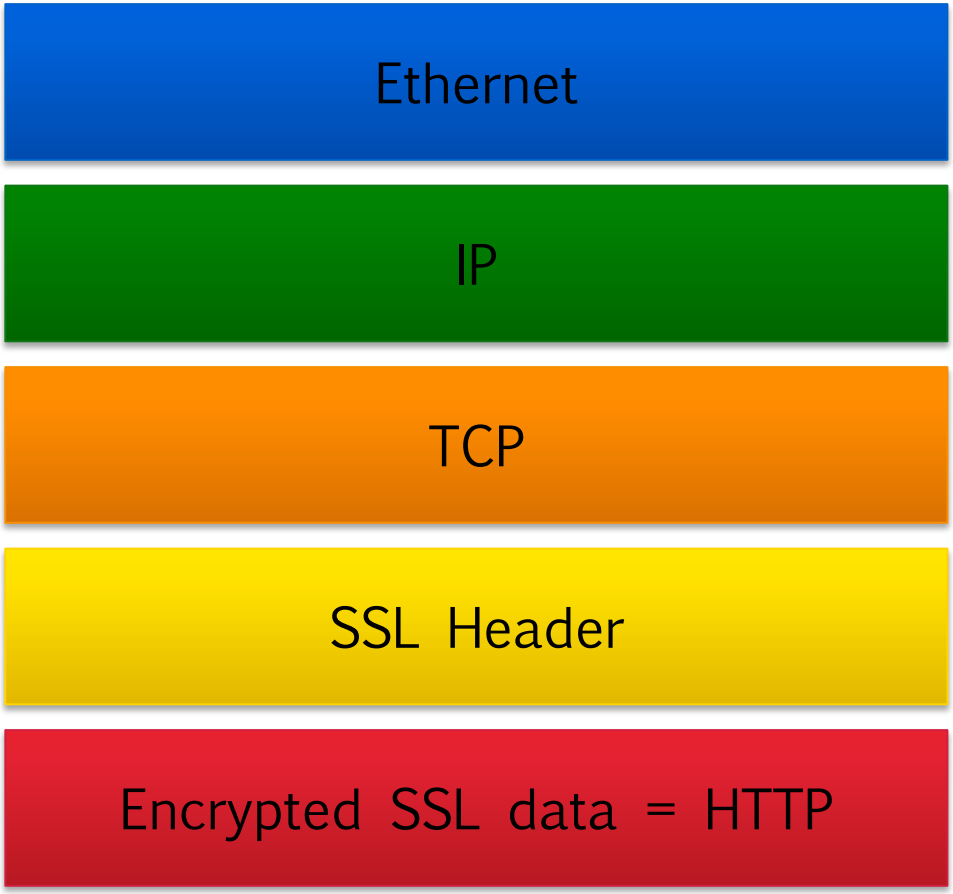
History

- Secure Sockets Layer was developed by Netscape in 1994 as a protocol which permitted persistent and secure transactions.
- In 1997 an Open Source version of Netscape's patented version was created, which is now OpenSSL.
- In 1999 the existing protocol was extended by a version now known as Transport Layer Security (TLS).
- By convention, the term "SSL" is used even when technically the TLS protocol is being used.

TLS/SSL : What it does

- Encryption
- Integrity
- Authentication

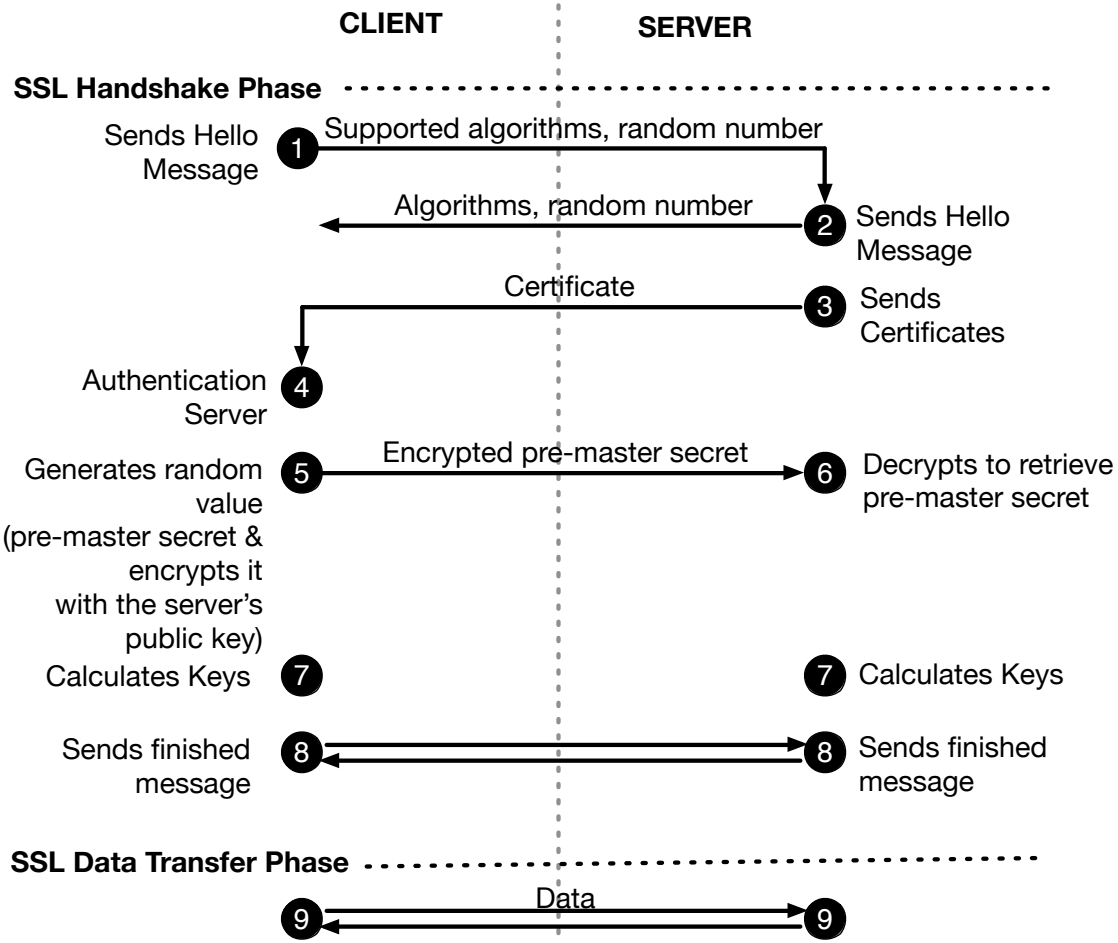
Location of SSL Protocol & TCP Ports



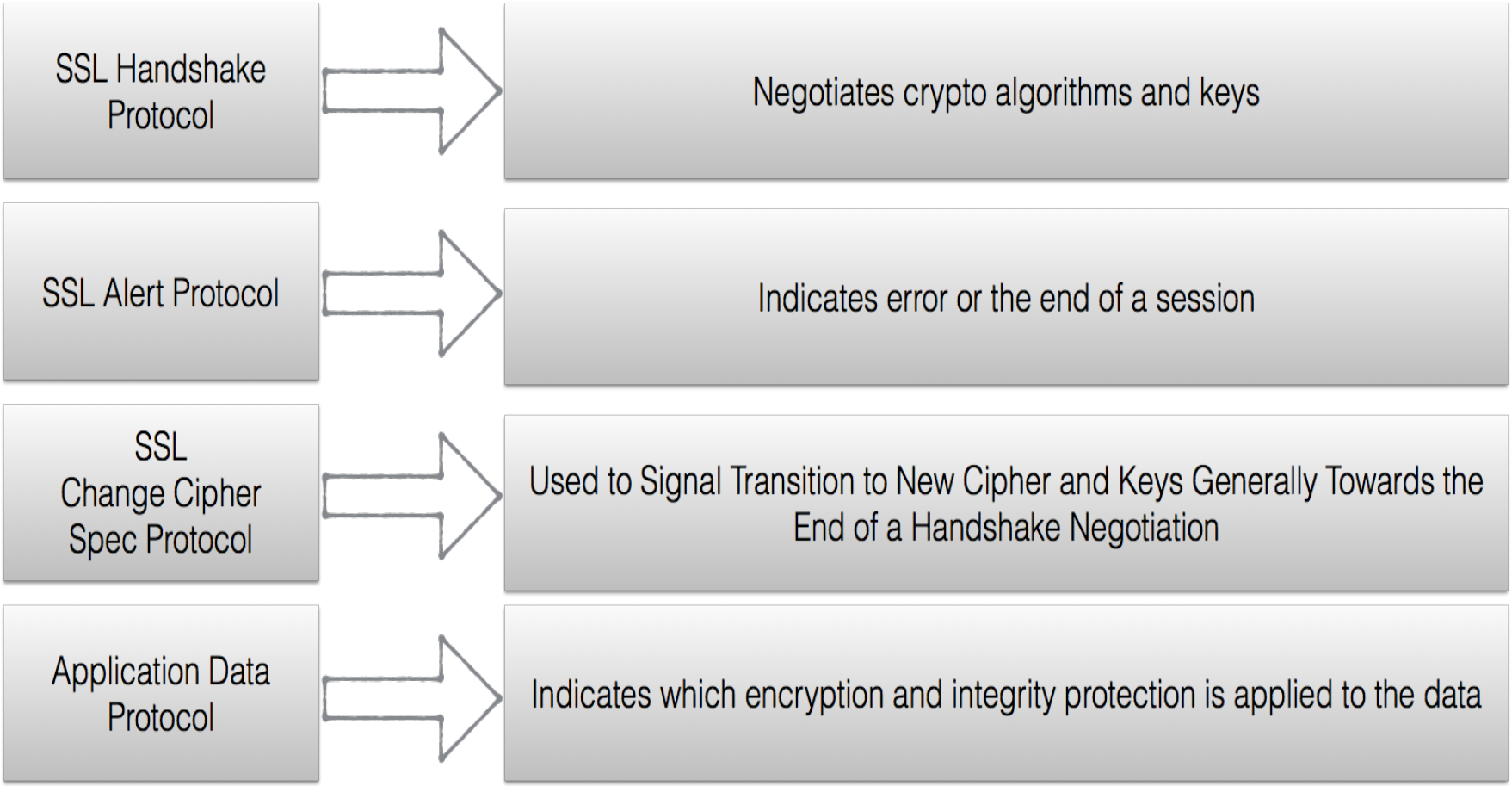
SSL Operations

- Application calls SSL connect routines to set up channel.
- Public Key cryptography is used during handshake to authenticate parties and exchange session key.
- Symmetric Key cryptography (using session key) is used to encrypt data.

How SSL Works



SSL Protocol Building Block Functions



SSL Handshake protocol

Key	Cipher	Hash
RSA	RC4	HMAC-MD5
Diffie-Hellman	Triple DES	HMAC-SHA
DSA	AES	

Version	3.3
Random Number	289484848484

Key	Cipher	Hash
RSA	RC4	HMAC-MD5
Diffie-Hellman	Triple DES	HMAC-SHA
DSA	AES	

SSL Alert Protocol

- Alert messages communicate the severity of the message and a description of the alert
- Fatal messages result in connection termination.

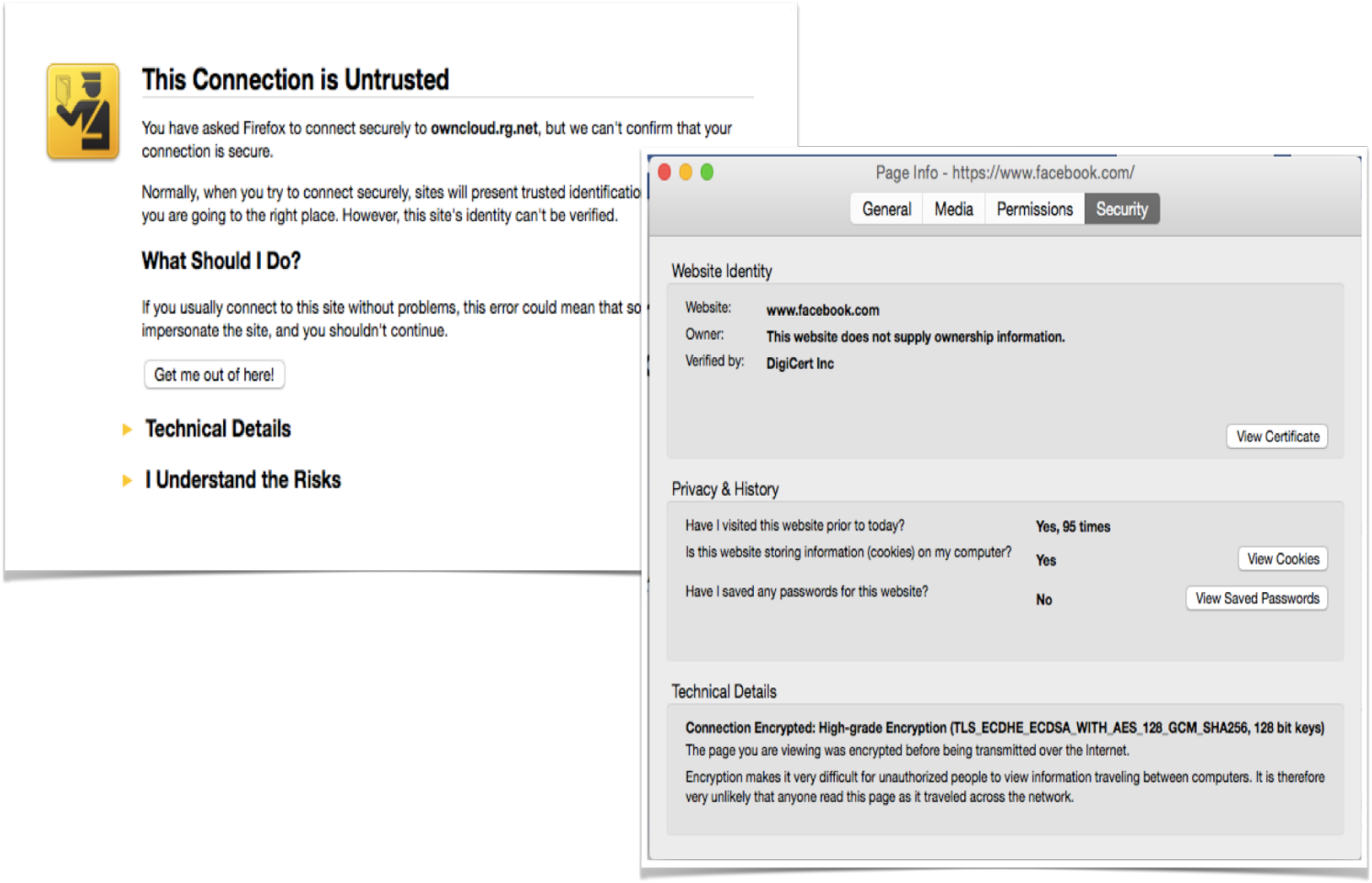
SSL ChangeCipherSpec Protocol

- The ChangeCipherSpec layer is composed of one message that signals the beginning of secure communications between the client and server.

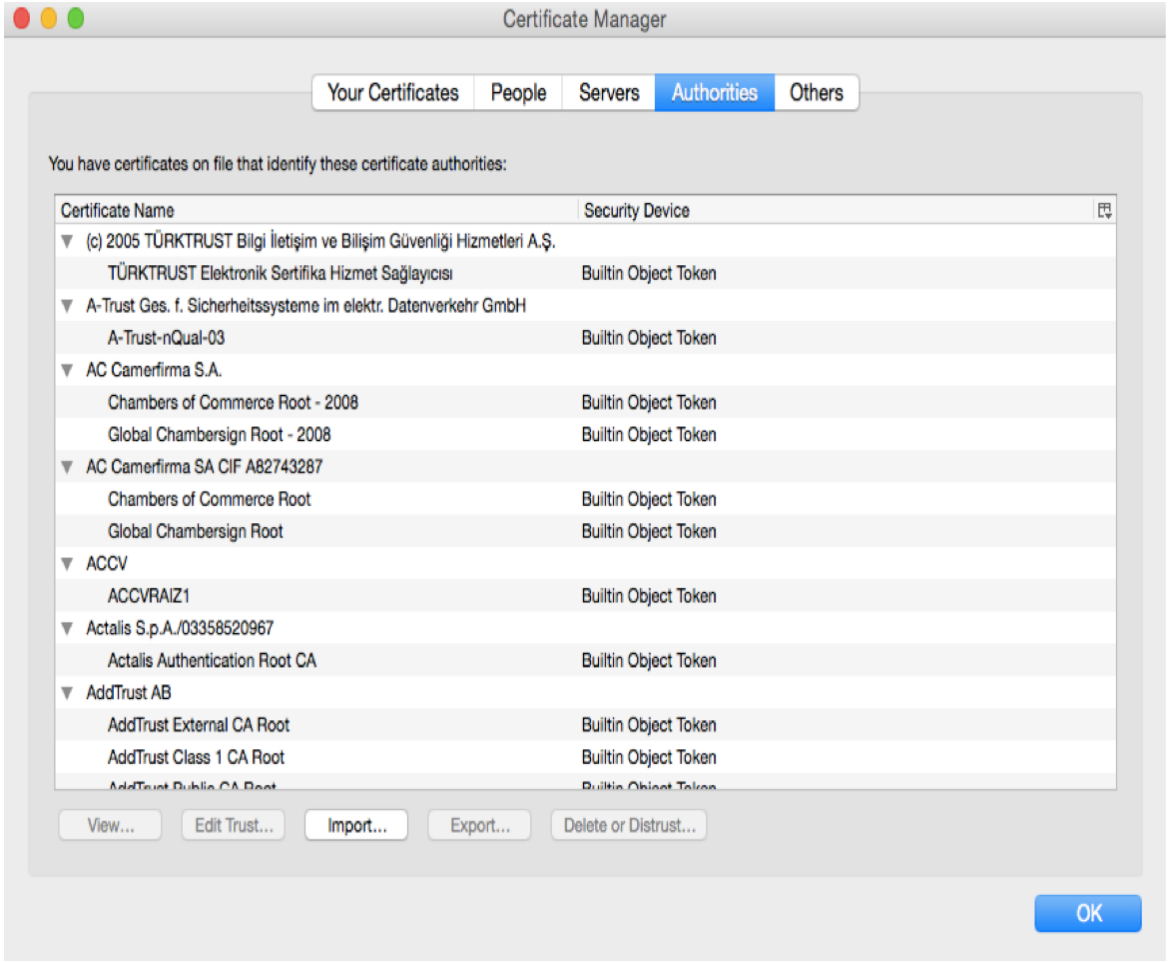
Application Data Protocol

- Application data messages are carried by the record layer and are fragmented, compressed, and encrypted based on the current connection state. The messages are treated as transparent data to the record layer.

Trusted vs Non Trusted Certificate



Certificate Authority



LAB