

# TLS/SSL

Securing your traffic



Fakrul Alam  
bdHUB Limited  
[fakrul@bdhub.com](mailto:fakrul@bdhub.com)

# 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

**Ethernet**

**IP**

**TCP**

**SSL Header**

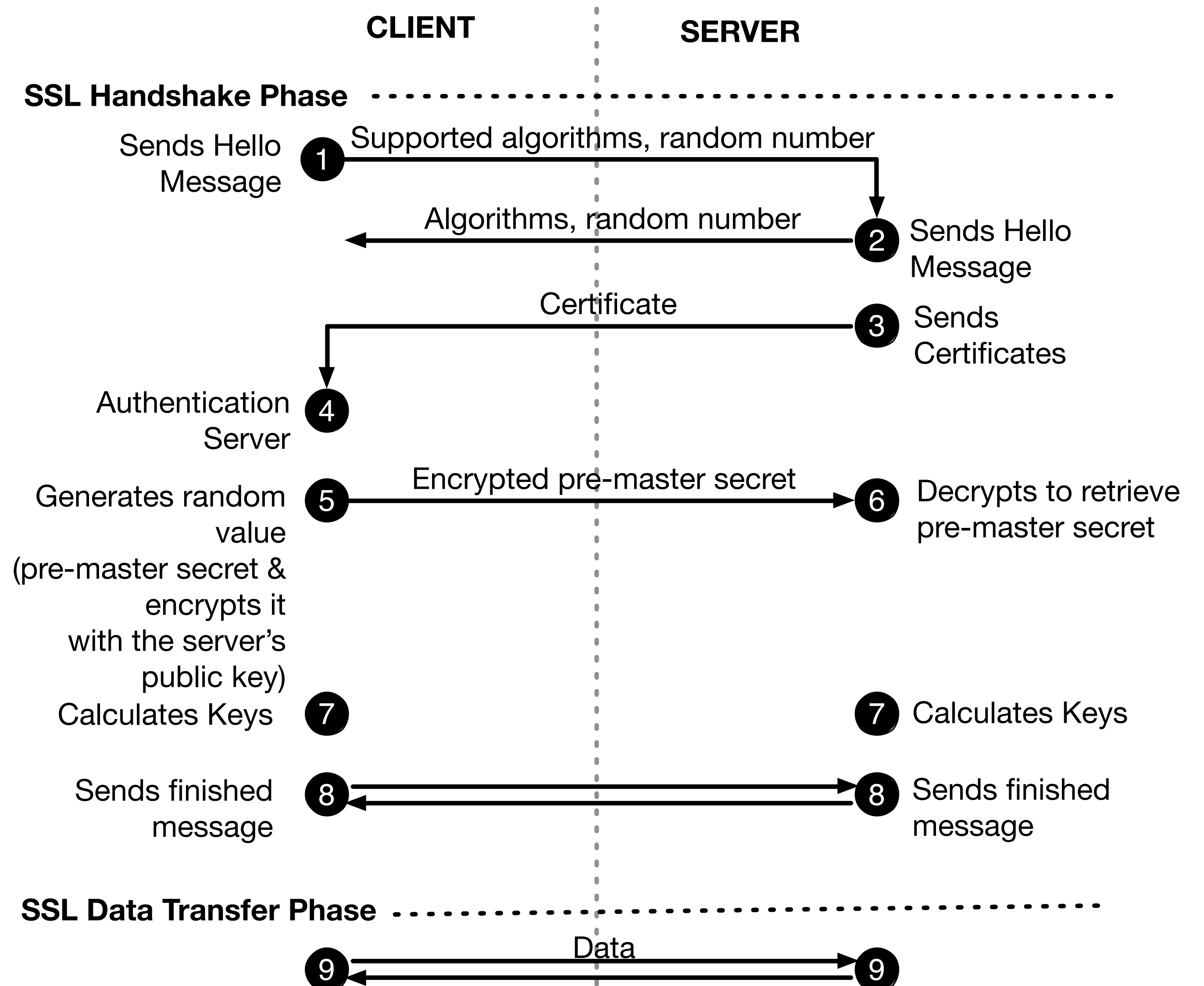
**Encrypted SSL data = HTTP**

- Independent of packet boundaries
- IANA has over 60 ports specified for SSL/TLS use. Some ports seen more than others
  - https 443
  - pop3s 995

# SSL Operations

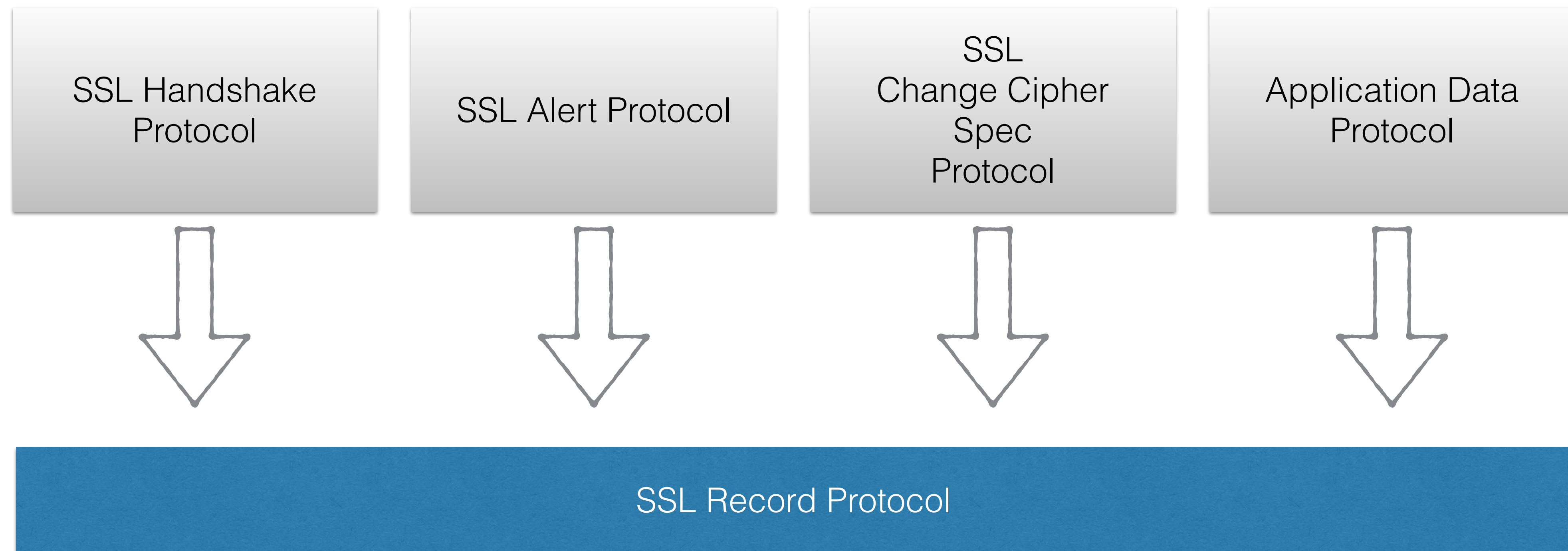
- Application calls SSL connect routines to set up channel
- **Public Key** cryptography is used during handshake to authenticate parties and exchange session key.
- **Symmetric Key** cryptography (using session key) is used to encrypt data.

# How SSL Works

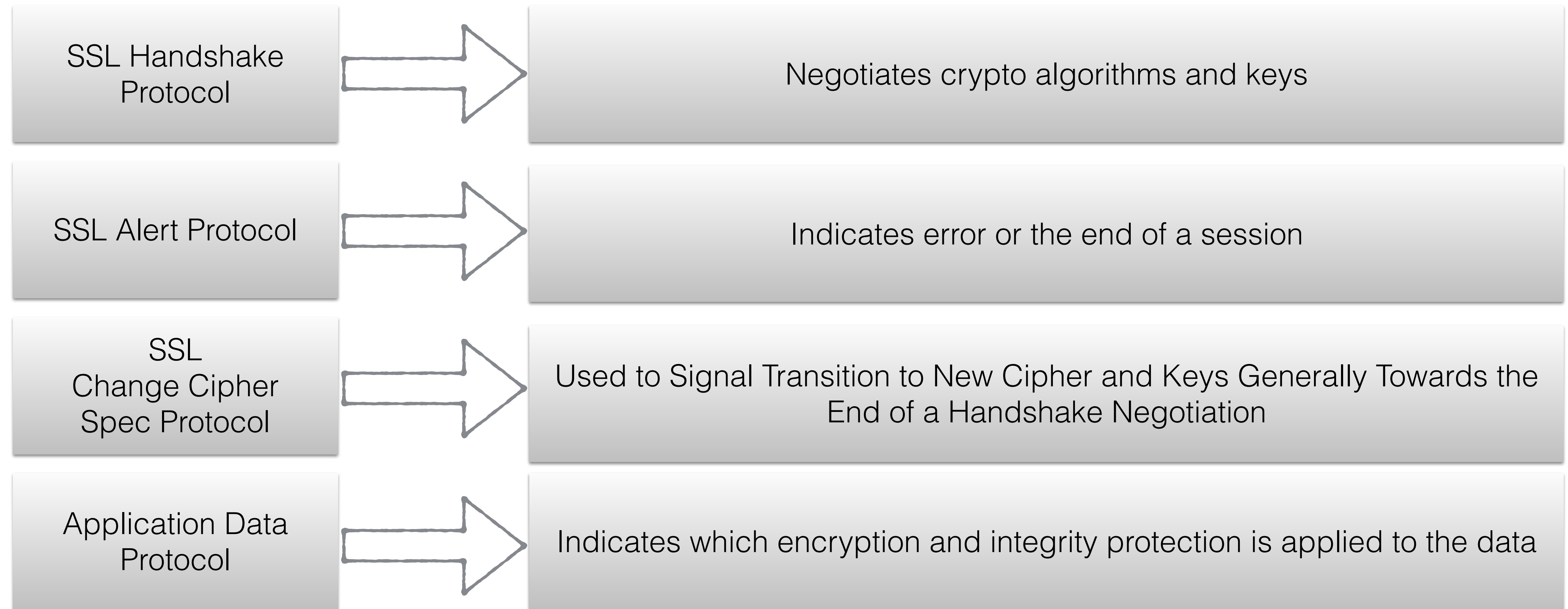


# SSL Protocol Building Blocks

- SSL is a Combination of a Primary Record Protocol with Four 'Client' Protocols



# 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



## This Connection is Untrusted

You have asked Firefox to connect securely to [www.facebook.com](#), but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification information to confirm you are going to the right place. However, this site's identity can't be verified.

### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is impersonating the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Page Info - <https://www.facebook.com/>

GeneralMediaPermissionsSecurity

Website Identity

Website:**www.facebook.com**

Owner:**This website does not supply ownership information.**

Verified by:**DigiCert Inc**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today?**Yes, 95 times**

Is this website storing information (cookies) on my computer?**Yes**[View Cookies](#)

Have I saved any passwords for this website?**No**[View Saved Passwords](#)

Technical Details

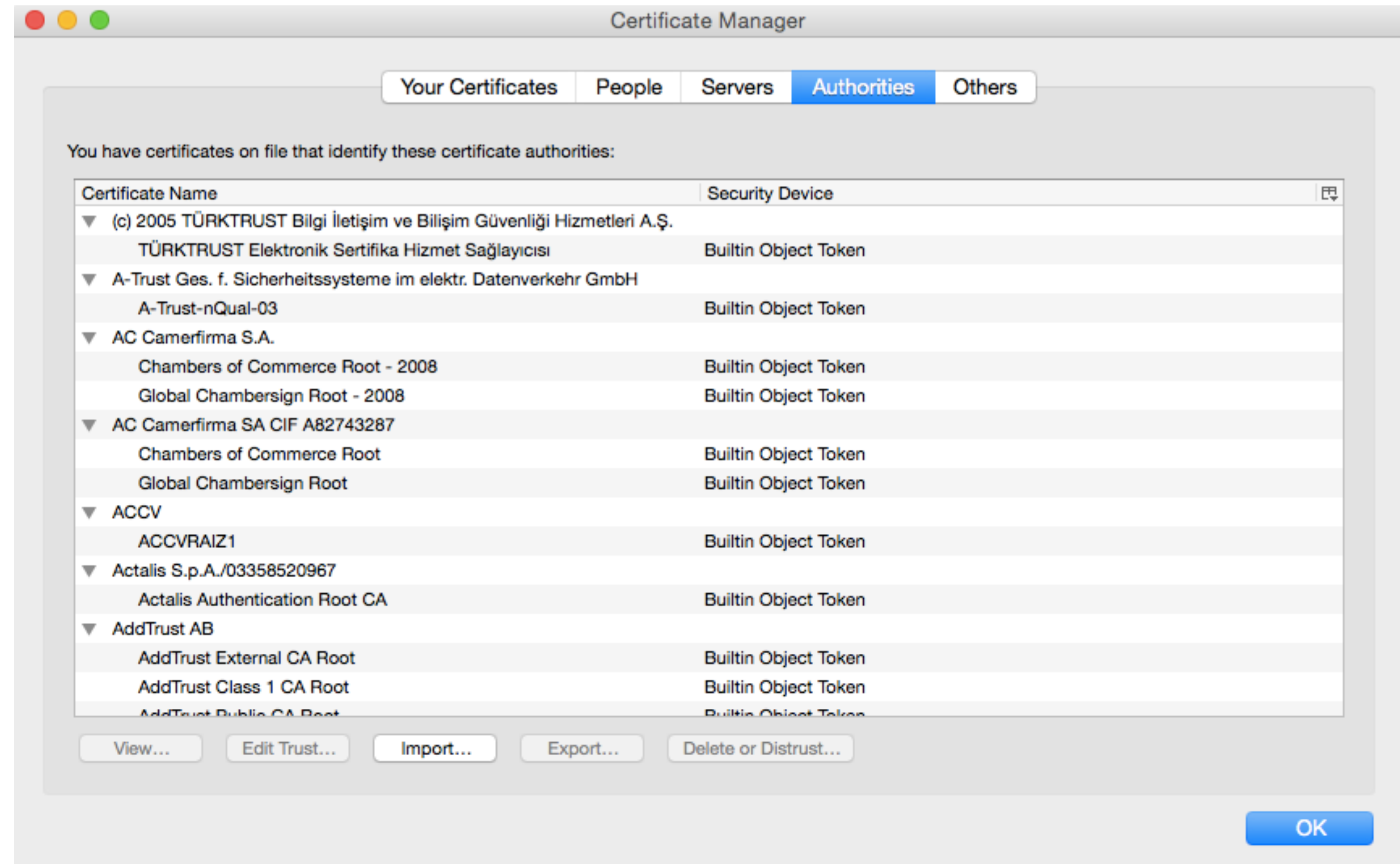
**Connection Encrypted: High-grade Encryption (TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, 128 bit keys)**

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

# Certificate Authority

- Someone both parties trust
- Issuer of Certificates
- Many standard ones listed in browser option
  - VeriSign
  - Comodo SSL
  - GlobalSign
  - Go Daddy
  - DigiCert



Question?