

Secure Socket Layer and Transport Layer Security

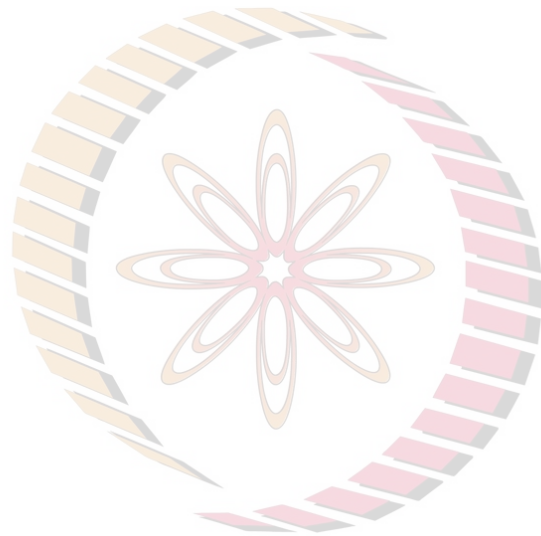
Dr. Neminath Hubballi

NPTEL

Overview

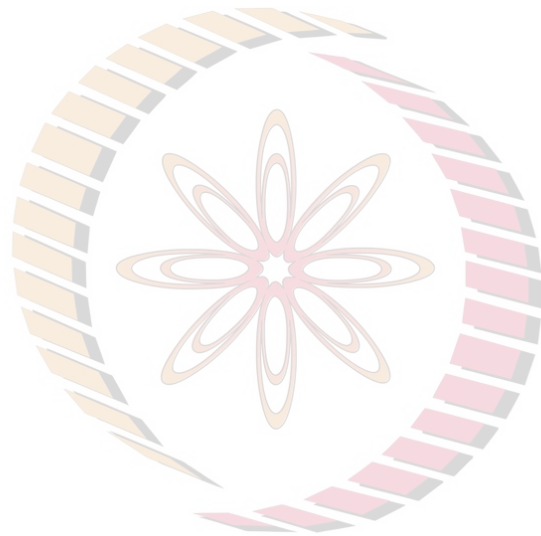
- ❑ Secure Socket Layer
 - ❑ Overview
 - ❑ Protocols
- ❑ Transport Layer Security
 - ❑ Differences with SSL
- ❑ Applications





NPTEL

Indian Institute of Technology Indore



NPTEL

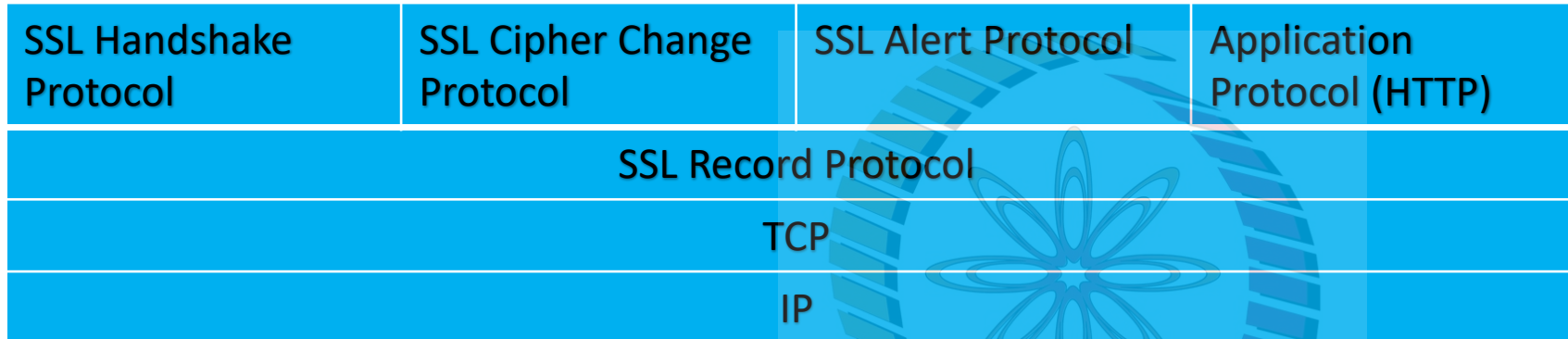
Indian Institute of Technology Indore

SSL/TLS Overview

- ☐ Provides reliable end-to-end secure service
- ☐ Authentication: Authenticate the communication end points
 - ☐ Deployment case: Only the server is authenticated
- ☐ Security: Confidentiality of data transferred over a channel
 - ☐ It does not encrypt the data but establishes a secure tunnel
- ☐ Application agnostic
- ☐ Prevent
 - ☐ Eavesdropping
 - ☐ Tampering
 - ☐ Forgery
- ☐ Works on top of TCP/IP and does not require changes to Operating System modules

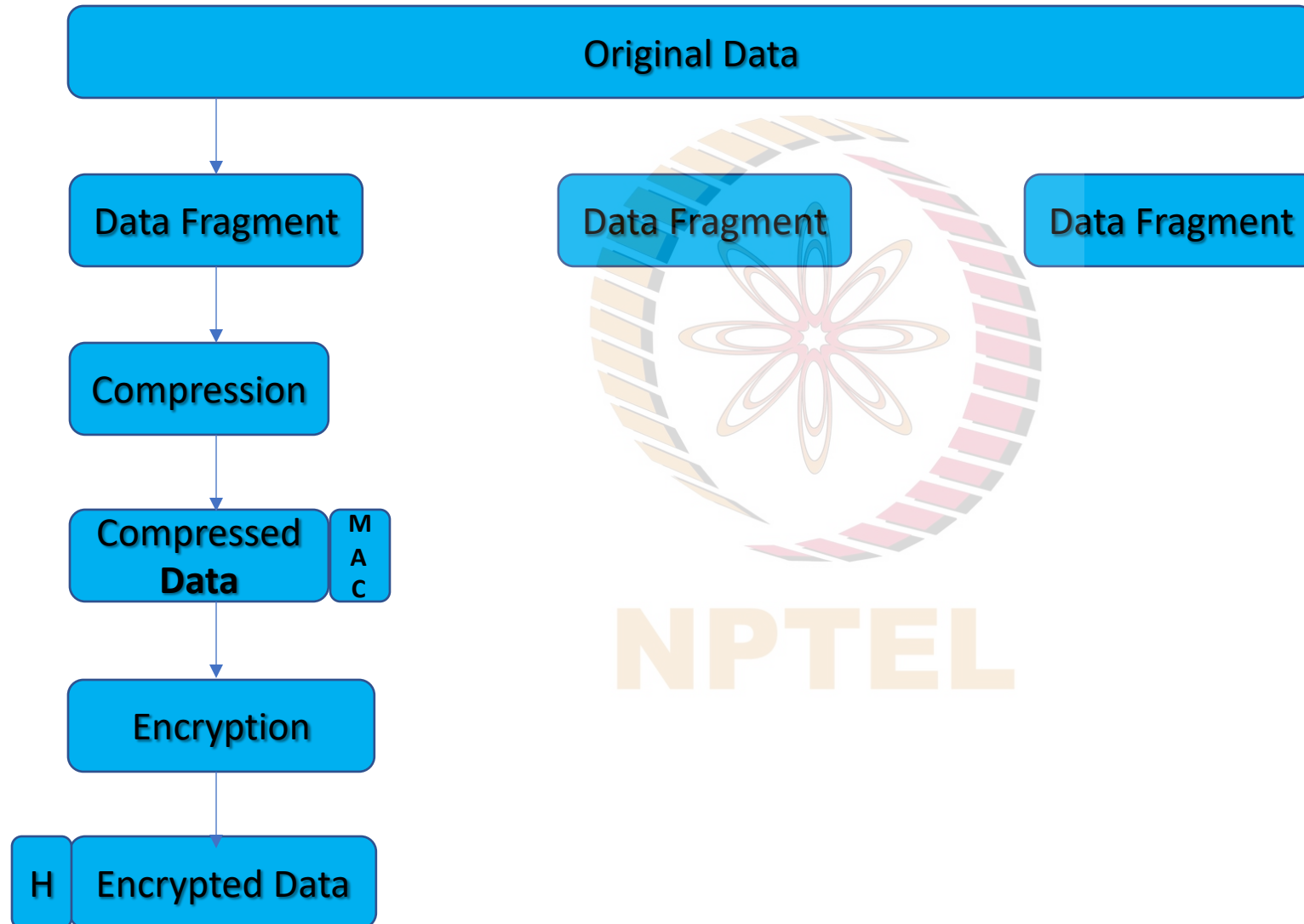
NPTTEL

SSL Layers

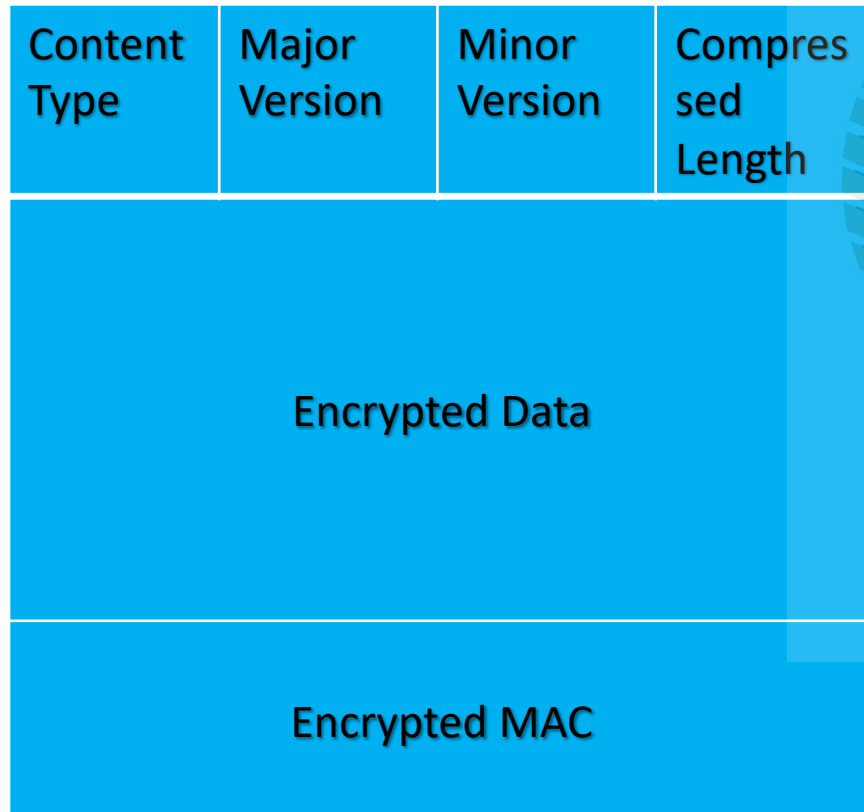


- ❑ SSL is a two layer protocol
- ❑ Layer-2 SSL Record Protocol
 - ❑ Provides basic security to application layer data
- ❑ Layer-1 has 3 sub protocols and are used for management of SSL

SSL Record Protocol Operation



SSL Record Protocol



- ❑ Content type (8 bits) - The higher layer protocol used to process the enclosed fragment.
- ❑ Major Version (8 bits) - Indicates major version of SSL in use. For SSLv3, the value is 3.
- ❑ Minor Version (8 bits) - Indicates minor version in use. For SSLv3, the value is 0.
- ❑ Compressed Length (16 bits) - The length in bytes of the compressed (or plaintext) fragment.
- ❑ Contents of record after header: data, padding, MAC
- ❑ MAC = hash {secret key, data+padding, sequence number}

SSL Alert Protocol

Warning/Fatal	Code
1 byte	1 byte

- ☐ unexpected_message
- ☐ bad_record_mac
- ☐ decompression_failure
- ☐ handshake_failure
- ☐ illegal_parameter

- ☐ Communicate errors both from Client/Server
- ☐ Errors during
 - ☐ Handshake
 - ☐ Processing data at server
- ☐ Compression and Encryption
 - ☐ As applicable for the session
- ☐ Fatal error- close the connection immediately

SSL Change Cipher Protocol

1

- ☐ Sent to close a pending session,
- ☐ Setting all the crypto parameters to be used in connections resulting from that session
- ☐ Compression and Encryption
 - ☐ As applicable for the session

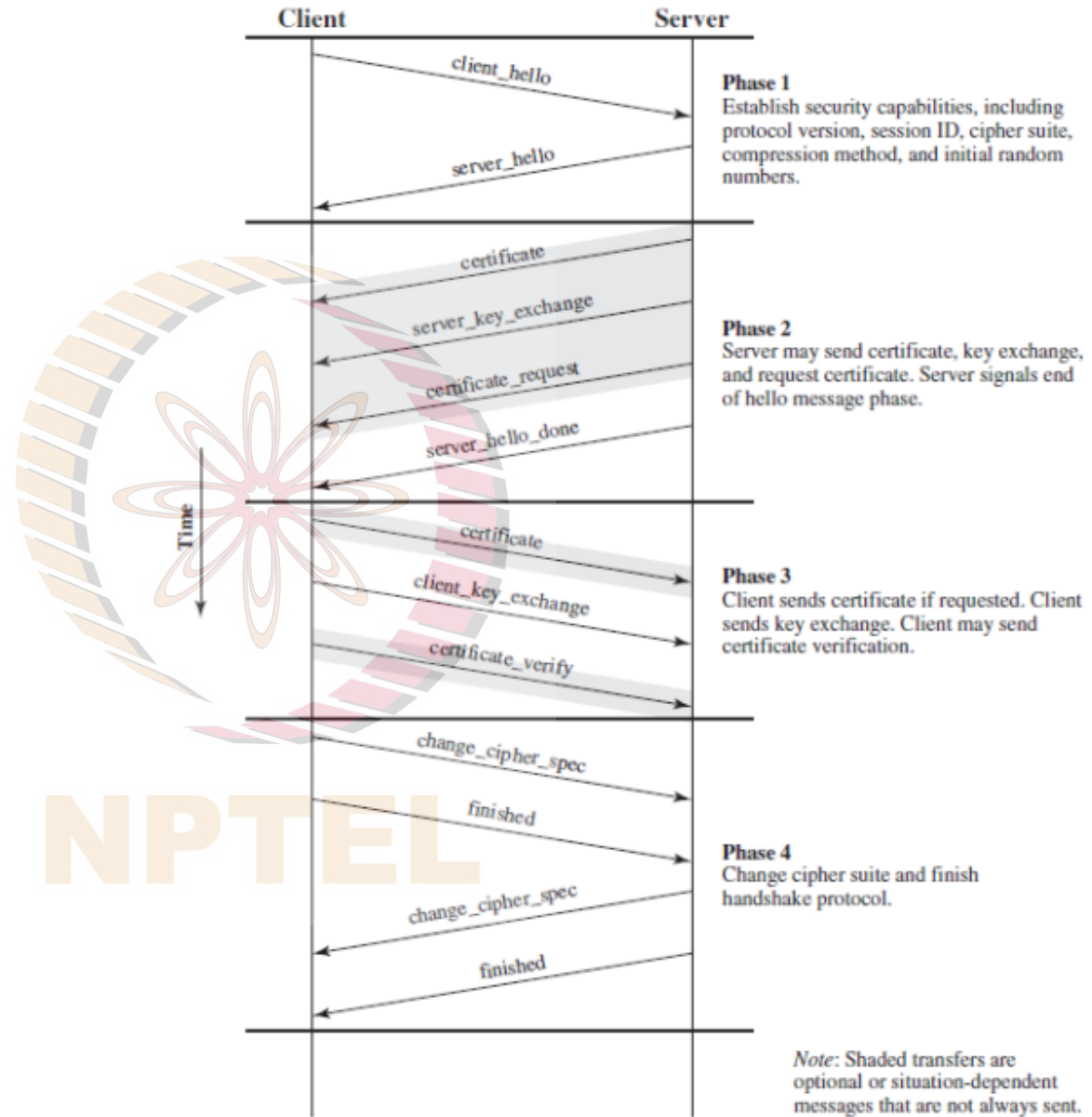
SSL Handshake Protocol

- ❑ Common format for the handshake message



SSL Handshake

□ Has four phases



SSL Handshake Phase-1



Ver	Highest Version that Client can Support
Random	32 bit timestamp + 28 bytes pseudorandom number
SessID	Variable length text
CipherSuite	Set of crypto algos supported by client + Preference
CompressionAlgo	The compression algorithm client understands

SSL Handshake Phase-1



Ver	Lowest Version that Server can Support
Random	32 bit timestamp + 28 bytes pseudorandom number
SessID	Variable length text –Same as client
CipherAccept	Set of crypto algos supported by client + Preference
CopressionAlgo	The compression algorithm client understands

SSL Handshake Phase-1

- ☐ Key Exchange Method: RSA, Fixed Diffie-Helman, Ephemeral Diffie-Helman, Anonymous Diffie-Helman, Fortezza
- ☐ Cipher Algorithm: RC4, RC2, DES, 3DES, DES40, IDEA
- ☐ MAC Algorithm: MD5, SHA-1
- ☐ CipherType: Stream, Block
- ☐ IsExportable: Yes/No
- ☐ HashSize: 0, 16(MD5), 20 (SHA-1) bytes
- ☐ Key Material: Data used for generating write keys
- ☐ IV Size: The size of initialization vector for block cipher chaining mode

SSL Handshake Phase-2



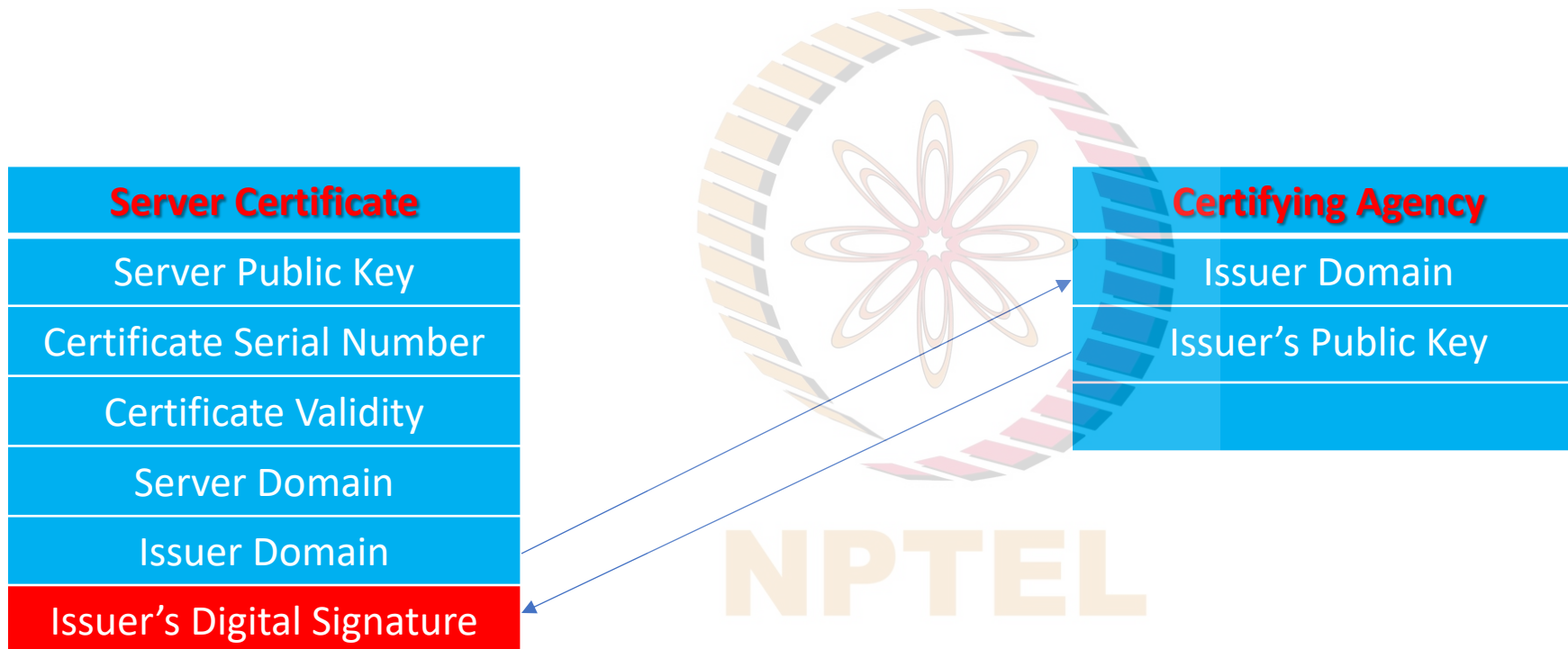
Certificate	Chain to the CA
Diffie-Helman Value	Optional
Request for Certificate from Client	Optional
Server Done	Completes this phase

SSL Handshake Phase-2



- ☐ Client verification
 - ☐ Validity of certificate
 - ☐ Check revocation list
 - ☐ CA credibility
 - ☐ CA public key

SSL Handshake Phase-2

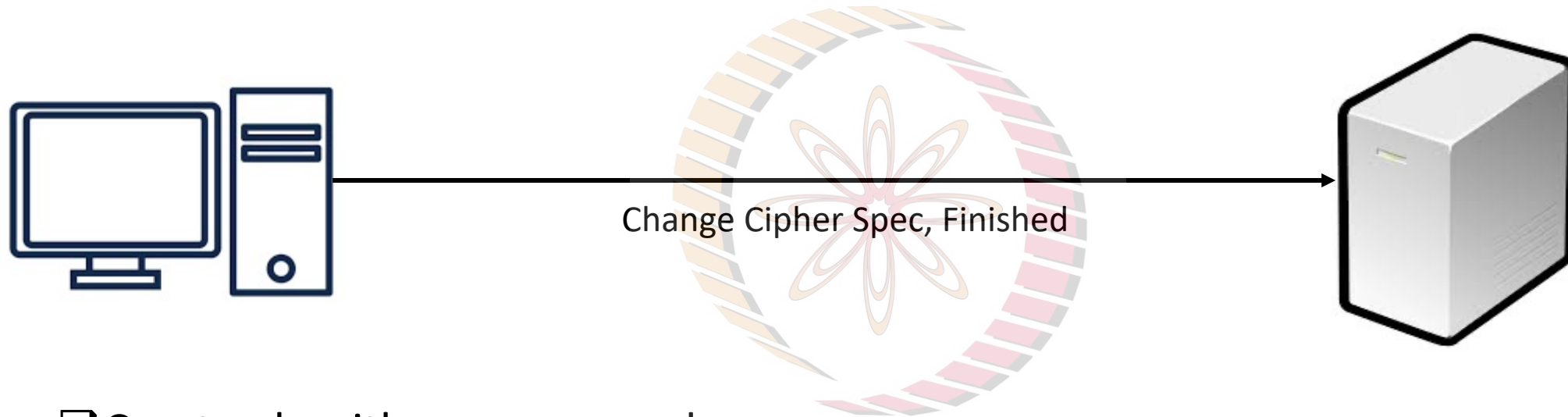


SSL Handshake Phase-3



- ❑ A secret S is encrypted with Server Public Key - server
- ❑ Key exchange message – key is delivered using key exchange method
- ❑ Send certificate to server – only if server has requested

SSL Handshake Phase-4



- ❑ Crypto algorithm now agreed
- ❑ Finished message: This message is encrypted with chosen algorithms and keys

SSL Handshake Phase-4



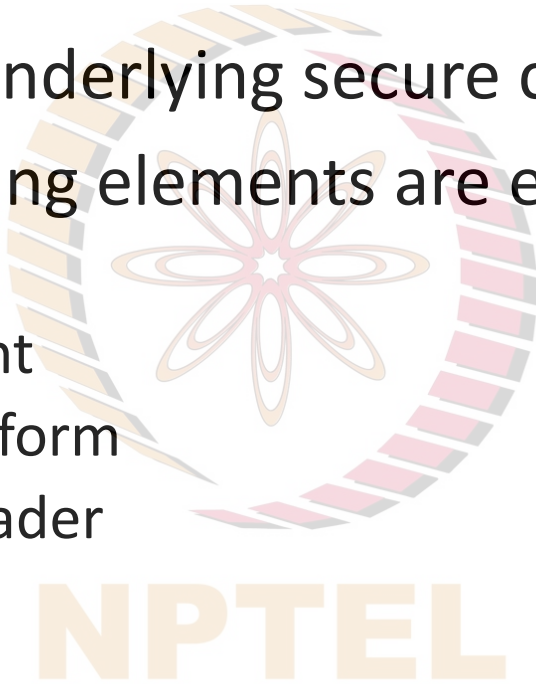
- ❑ Finished message: This message is encrypted with chosen algorithms and keys. This is the same message as sent by client

Transport Layer Security (TLS)

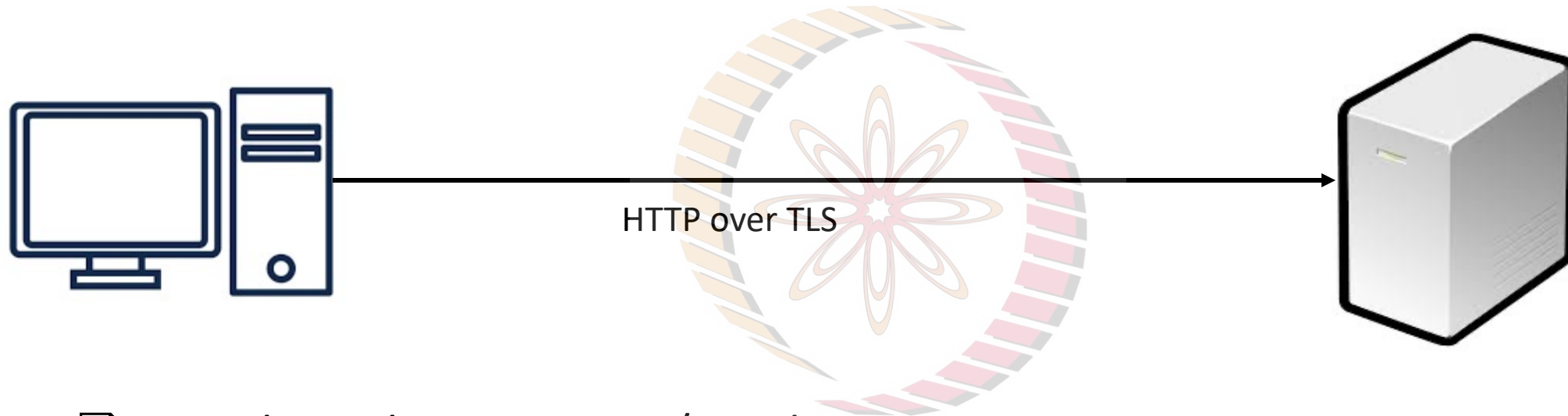
- ❑ Is an IETF standard
- ❑ Record protocol - major and minor versions 3
- ❑ HMAC $\text{HMAC}_K(M) = H[(K^+ \oplus \text{opad}) \parallel H[(K^+ \oplus \text{ipad}) \parallel M]]$
- ❑ SSL uses security from the beginning but TLS starts with plain communication and switches to secured communication
- ❑ TLS is not backward compatible with SSL
- ❑ Adds many more alert messages

HTTPS

- ☐ HTTPS uses SSL/TLS as underlying secure communication
- ☐ If SSL/TLS is used following elements are encrypted
 - ☐ URL of the document
 - ☐ Contents of the document
 - ☐ Contents of the browser form
 - ☐ Contents of the HTTP header
 - ☐ Cookies exchanged

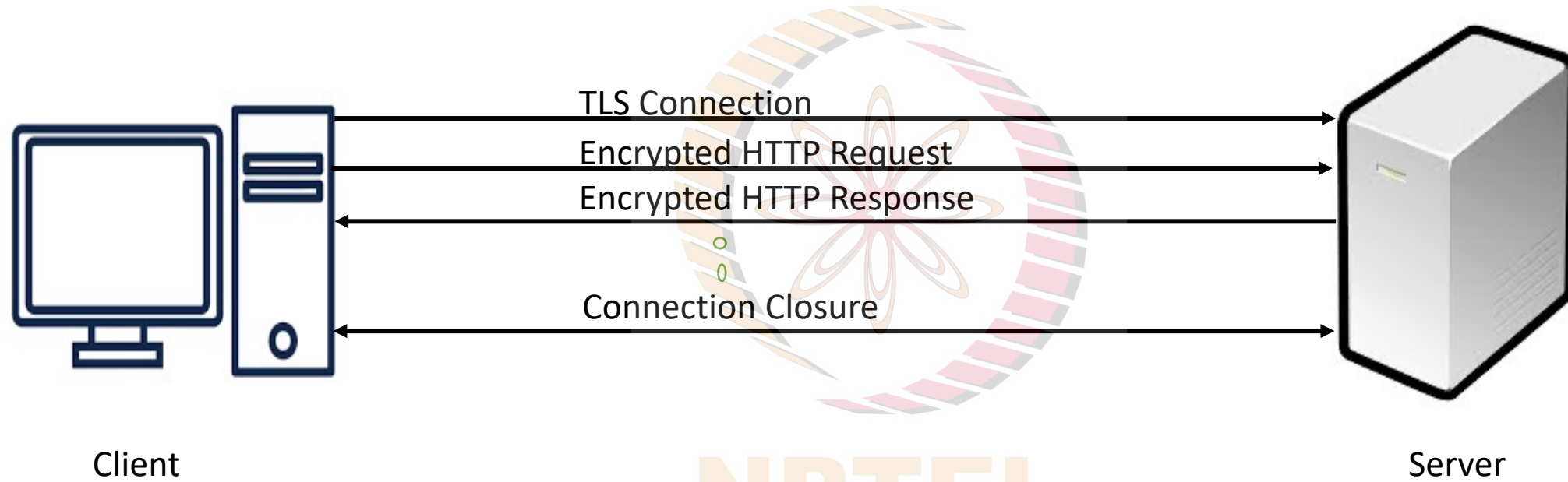


HTTP



- ❑ HTTP client also acts as TLS/SSL client
- ❑ Before any HTTP request is made, TLS connection is established
- ❑ A client-server pair can have more than one TCP/TLS connections between them

HTTP Connection over SSL



NPTEL

Secure Socket Layer Attacks

- ☐ SYN flood is possible
- ☐ TCP handshake is followed by SSL handshake
 - ☐ SSL Handshake is computationally expensive
- ☐ Regeneration of encryption method
 - ☐ Repeated requests

