Web Protocols

HTTP /2

HTTP/2

- a major revision of the HTTP.
  - Approved as a Proposed Standard on February 17, 2015.
- standardization effort supported by most major browsers
  - HTTP/2 support added by the end of 2015.
- As of Sep 2019, 40.7% of top 10 million websites supported HTTP/2*

* *World Wide Web Technology Surveys*. W3Techs. Retrieved September 1, 2019

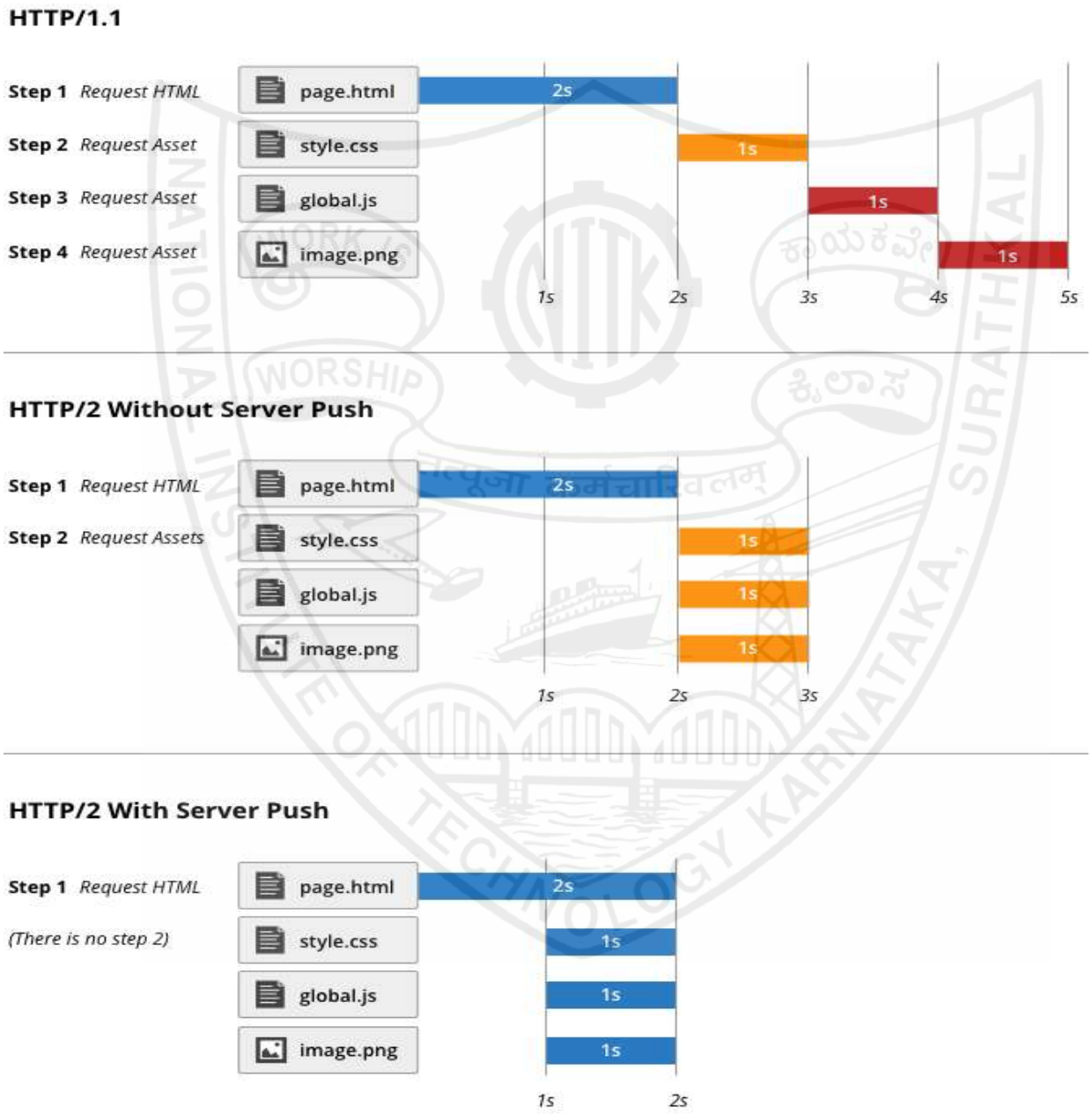
HTTP/2 Capabilities

- **Maintain high-level compatibility with HTTP 1.1**
  - All methods, status codes, and URIs, and most header fields supported.
- **Negotiation mechanism**
  - Allows Web clients and servers to elect to use HTTP 1.1, 2.0, or potentially other non-HTTP protocols.
- **Decrease latency**
  - improve page load speed in web browsers by introducing new features.

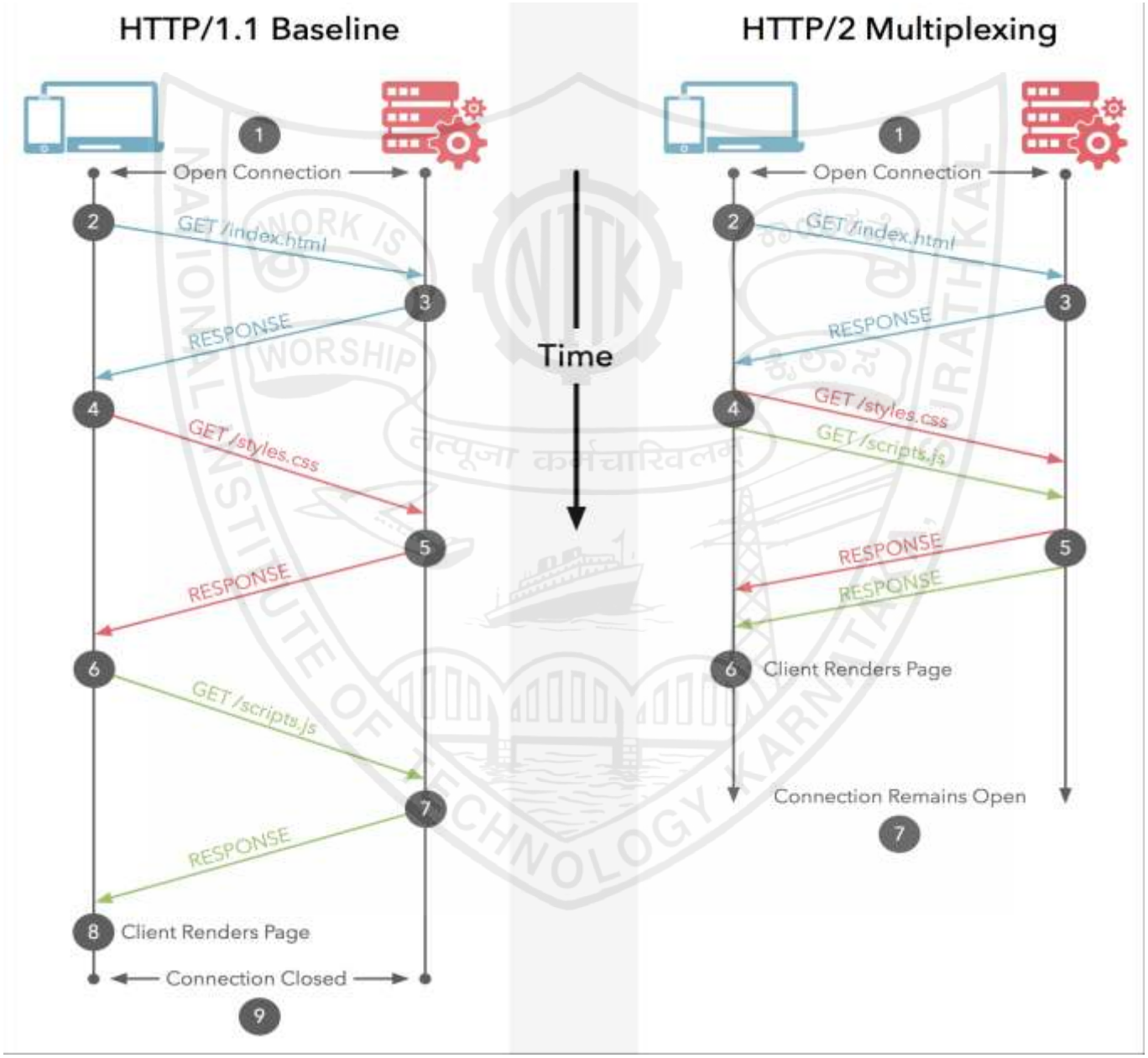
HTTP/2 – New Features

- HTTP/2 Server Push
- Multiplexing multiple requests over a single TCP connection
- Fixing the head-of-line blocking problem in HTTP 1.x
- Support for desktop web browsers, mobile web browsers, web APIs, web servers at various scales, proxy servers, reverse proxy servers, firewalls, and content delivery networks.

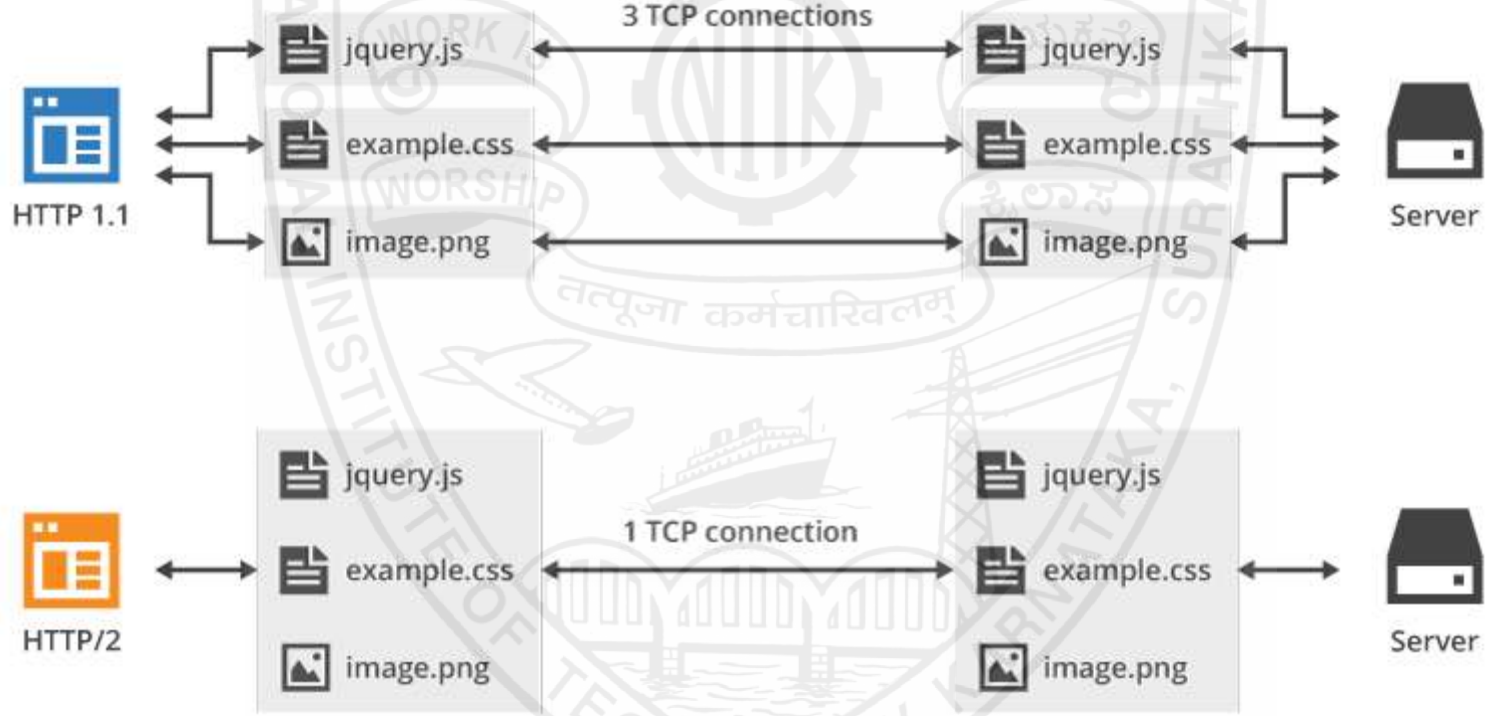
HTTP/2.0 New Features - Server Push



HTTP/2.0 New Features - Multiplexing

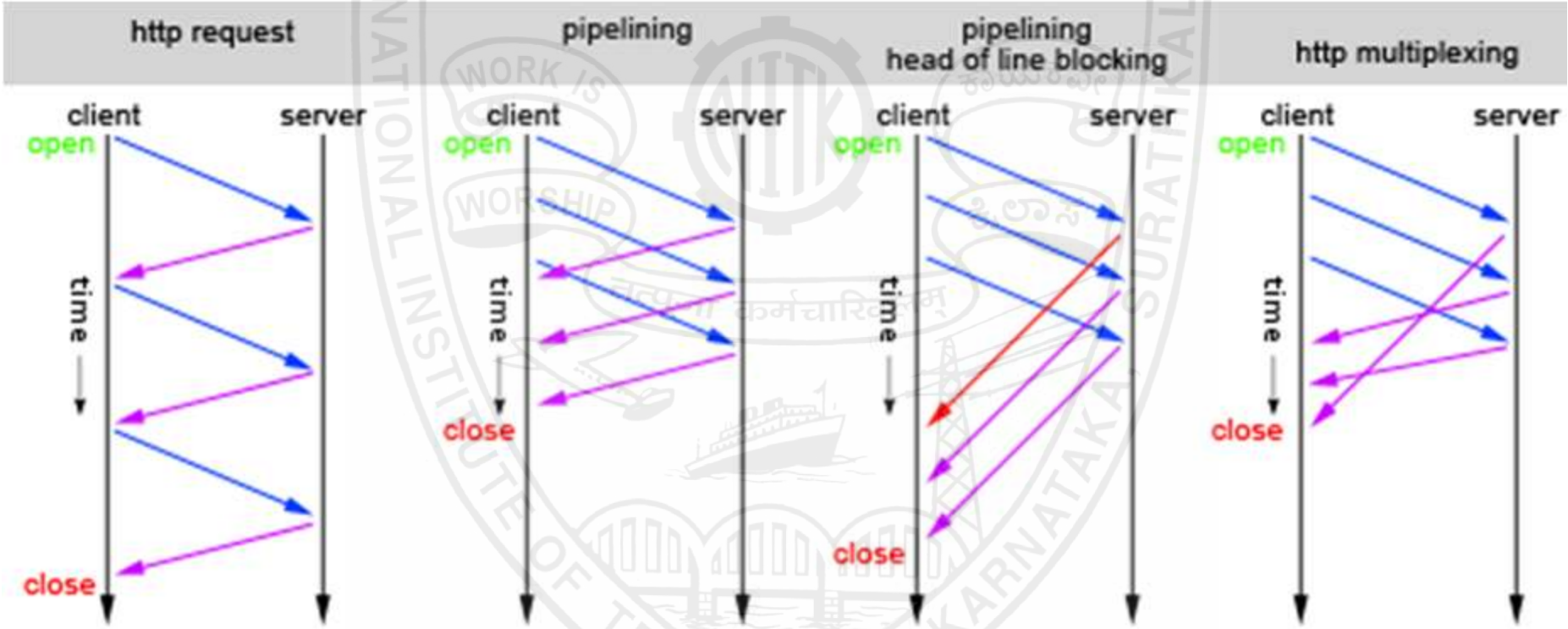


HTTP/2.0 New Features
- Addressing Head-of-Line Blocking



HTTP/2.0 New Features

Multiplexing & Addressing Head-of-Line Blocking



HTTP/2.0 New Features

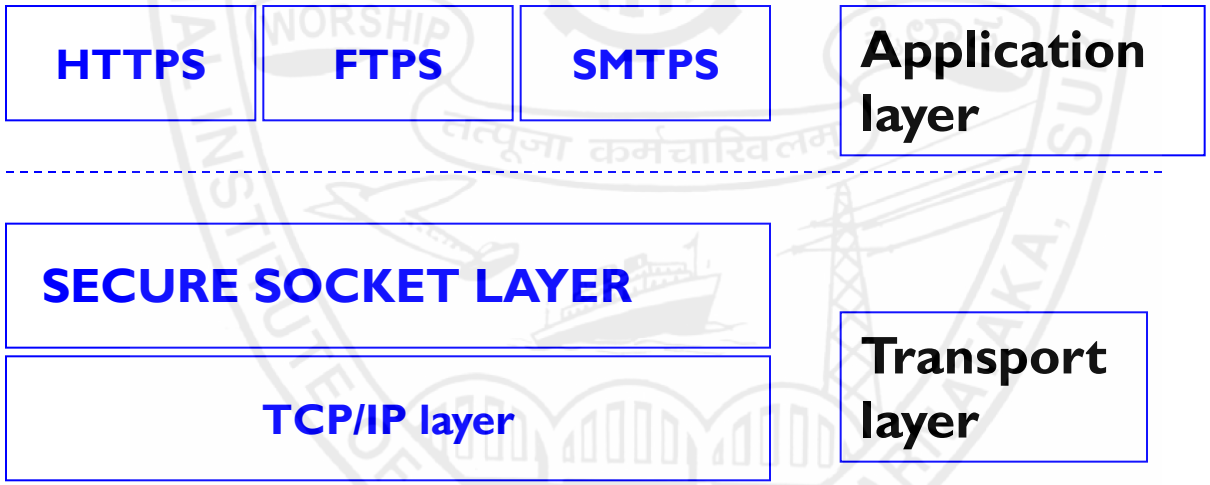
- Support for
  - Desktop web browsers
  - Mobile web browsers
  - Web APIs
  - Web servers at various scales
  - Firewalls
  - Proxy servers
  - Reverse proxy servers
  - Content delivery networks.

Web Protocols

HTTPS

HTTPS

- Acronym for HTTP over SSL, HTTP over TLS and HTTP Secure.
- Utilizes the **Secure Sockets Layer** meta-protocol over TCP/IP.

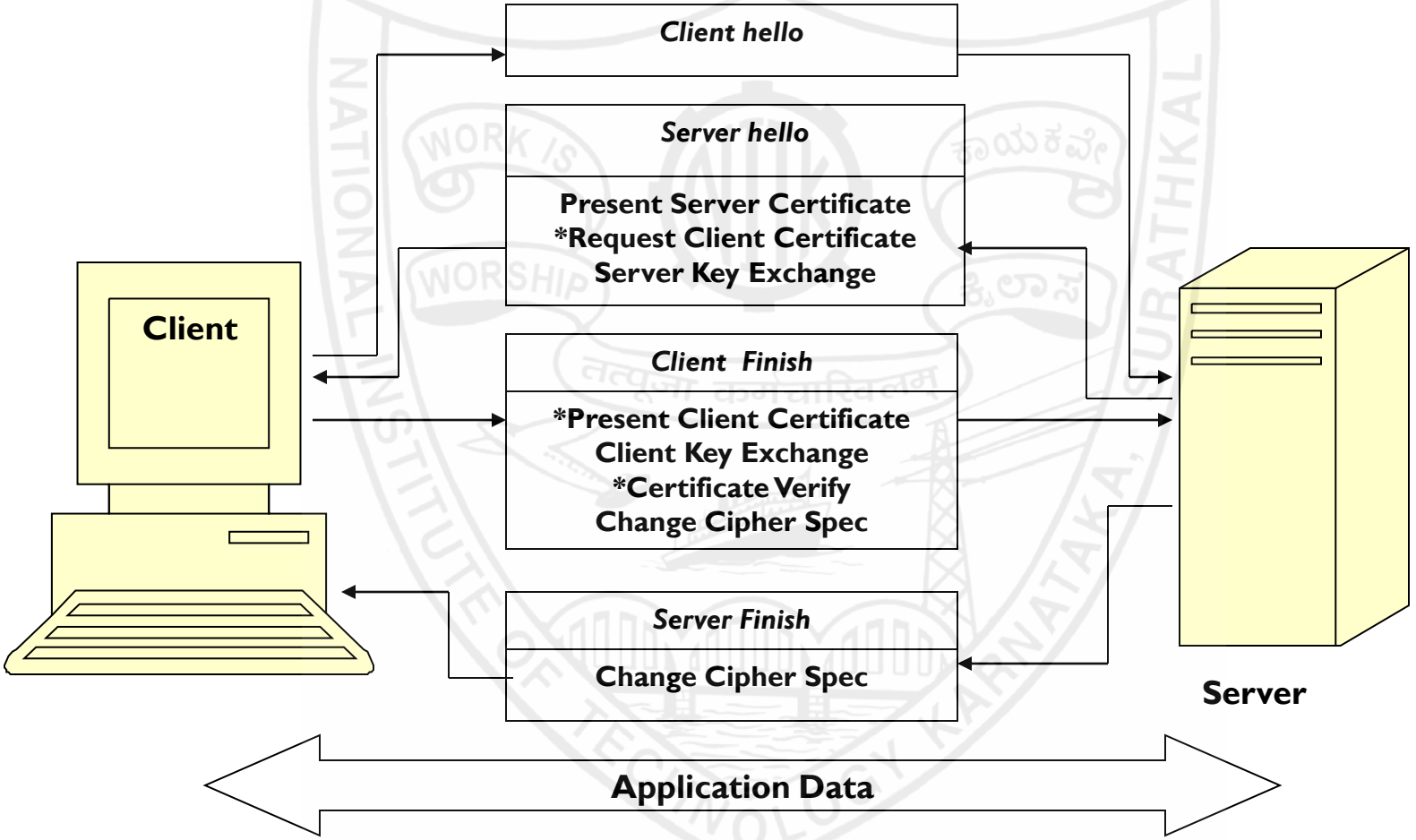


- SSL/TLS connection uses a dedicated TCP/IP socket (e.g. port 443 for https)

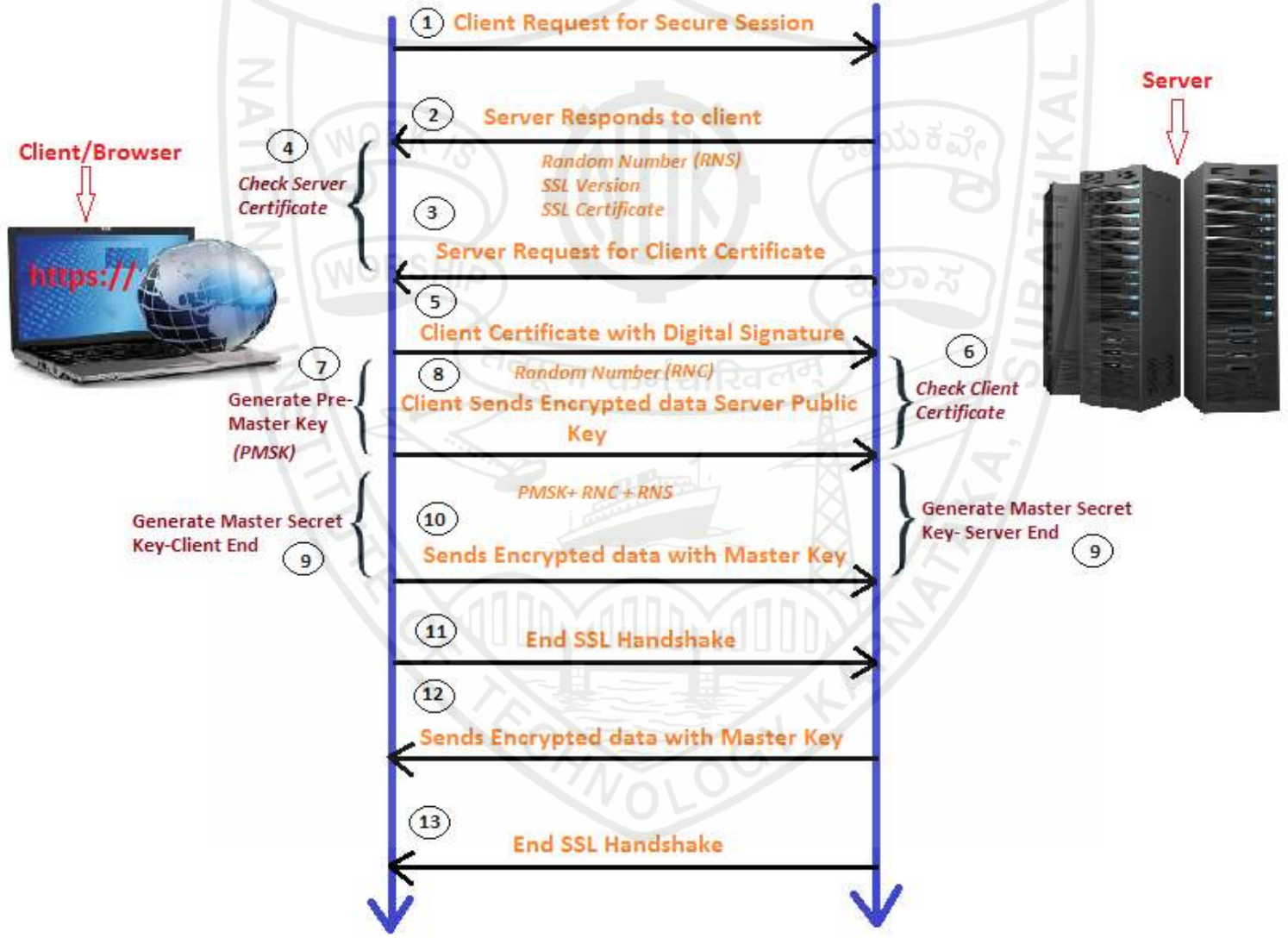
HTTPS - Objectives

- **Authentication** of the web site and associated web server
  - preventing Man-in-the-middle attacks
- **Integrity:** Bidirectional encryption of communications between a client and server,
  - protect against tampering with and/or forging the contents of communication.
- **Confidentiality:** ensuring that communication remains confidential.
- **Verification and Non-repudiation:** reasonable guarantee that one is communicating with precisely the web site that one intended to communicate with (as opposed to an impostor)

SSL Handshake



Working of HTTPS



Working of HTTPS

- A browser requests a secure page (usually https://).
- The web server sends its public key with its certificate.
- Browser checks that the certificate was issued by a trusted party (usually a trusted root CA), that the certificate is still valid and that the certificate is related to the site contacted.
- Browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data.
- Web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data.
- Web server sends back the requested html document and http data encrypted with the symmetric key.
- Browser decrypts the http data and html document using the symmetric key and displays the information.

Certificate Authority (CA)

- a trusted third party organization that is used by both interacting parties.
  - issues digital certificates.
- Digital certificate –
  - certifies the ownership of a public key by the subject named on the certificate.
  - allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified.
- Some CA companies – Verisign, Thawte, GlobalSign, GeoTrust etc.

Certificate Authority (CA)

- Certification Authority Functions:
  - Accept applications for certificates.
  - Thoroughly verify the identity of the person/organization etc applying for the certificate.
  - Issue certificates.
  - Revoke/Expire certificates.
  - Provide status information about the certificates that it has issued.

Digital certificates

- A digital file that certifies the identity of an individual or institution, or even a router seeking access to digital information stored on a computer/device.

- issued by a Certification Authority, and serves the same purpose as a driver's license or a passport.

Digital certificates (contd.)

- Contents -
  - name of the certificate holder,
  - a serial number,
  - expiration dates,
  - a copy of the certificate holder's public key (used for encrypting messages and digital signature)
  - the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

Digital Certificates (contd.)

- Four main types of digital certificates:
  1. Server Certificates
  2. Personal Certificates
  3. Organization Certificates
  4. Developer Certificates

Digital Certificates (contd.)
Basic Certs

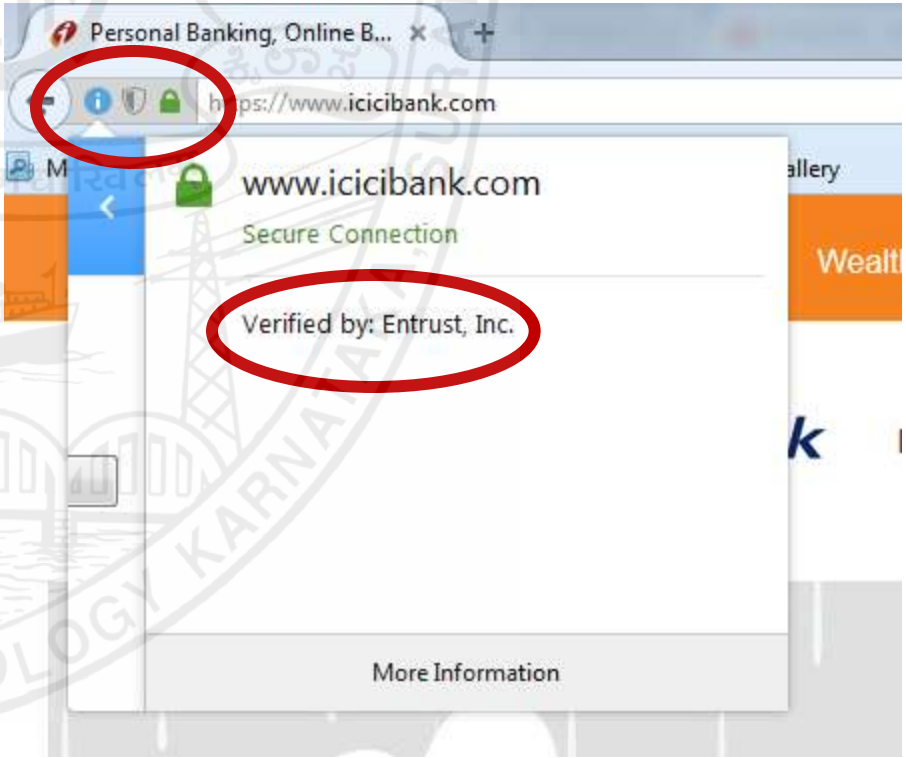
- All elements on the page fetched using HTTPS (with some exceptions)
- For all elements:
  - HTTPS cert is issued by a CA trusted by *browser*
  - HTTPS cert is *valid* (e.g. not expired)
  - *CommonName* in cert matches domain in URL.

The lock UI: help users authenticate site

- Firefox 3:

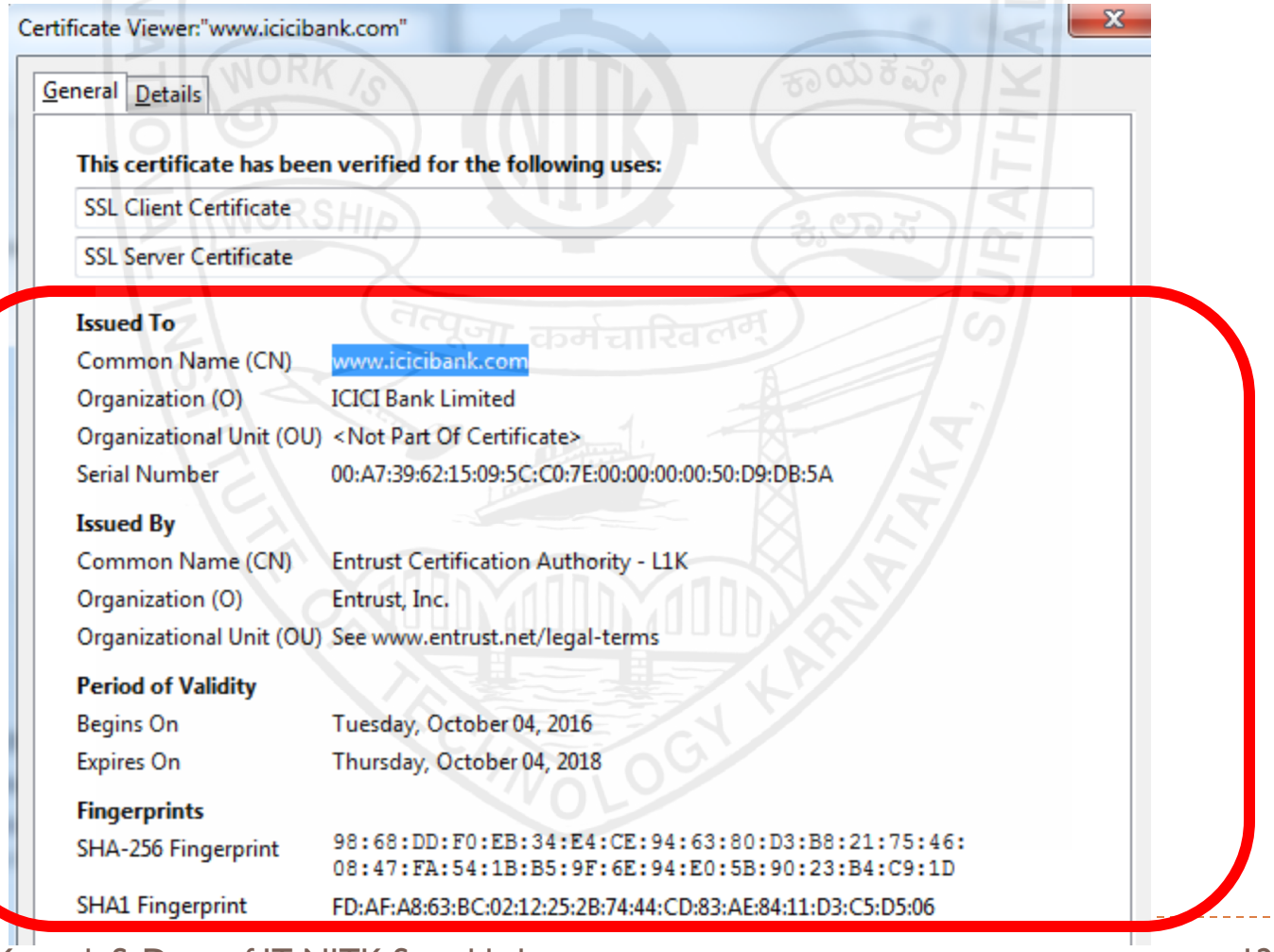
(no SSL)

(SSL)



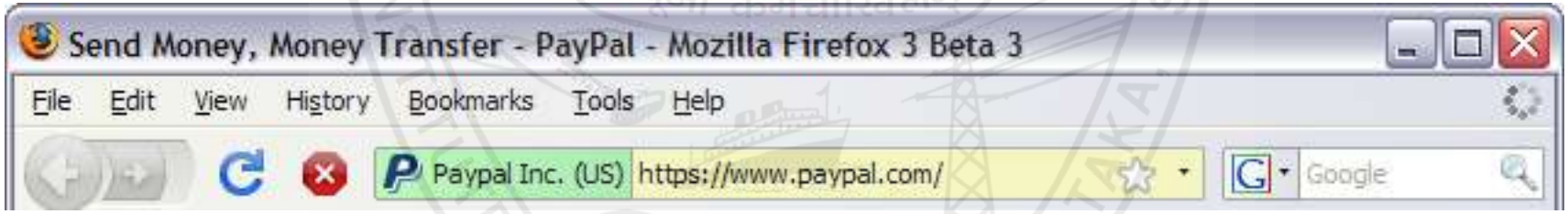
The lock UI: help users authenticate site

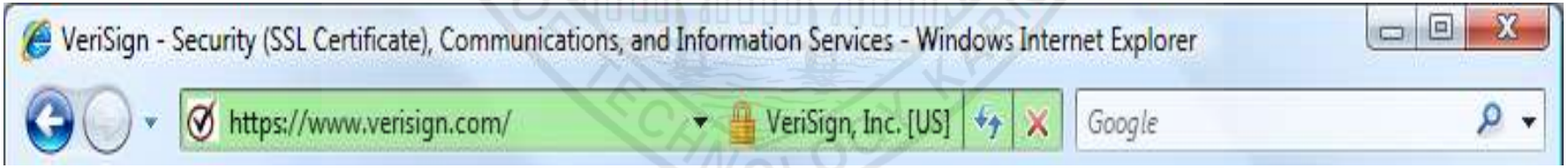
- Firefox 3: clicking on bottom lock icon gives additional info…

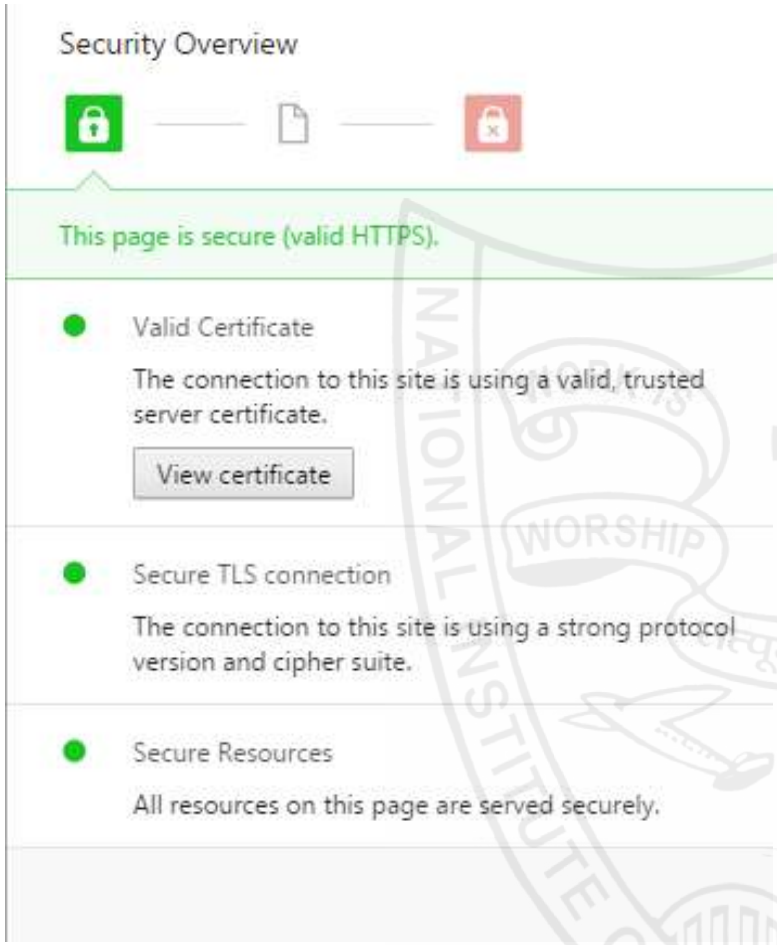


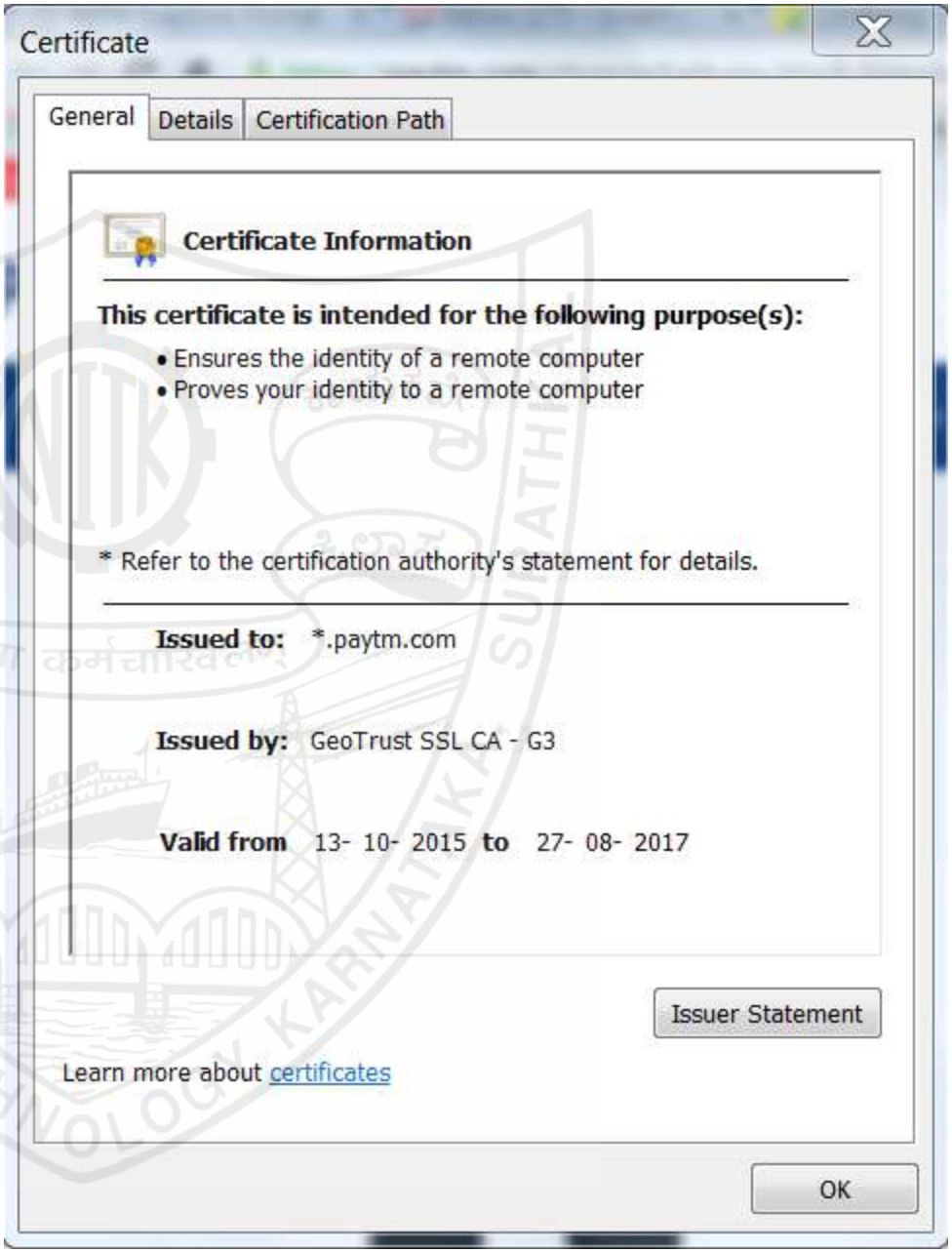
Digital Certificates (contd.)
Extended Validation (EV) Certs

- Harder to obtain than regular certs
  - requires human lawyer at CA to approve cert request
- Designed for banks and large e-commerce sites
  - Helps block "semantic attacks": www.iciciibank.com






Security Overview
This page is secure (valid HTTPS).
Valid Certificate
The connection to this site is using a valid, trusted server certificate.
View certificate
Secure TLS connection
The connection to this site is using a strong protocol version and cipher suite.
Secure Resources
All resources on this page are served securely.


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.paytm.com
Issued by: GeoTrust SSL CA - G3
Valid from 13- 10- 2015 to 27- 08- 2017
Issuer Statement
Learn more about certificates
OK

HTTP vs. HTTPS...

- HTTP URLs begin with "http://" and use port 80 by default.
  - HTTPS URLs begin with "https://" and use port 443 by default
- HTTP is insecure and is subject to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information.
  - HTTPS is designed to withstand such attacks and is considered secure against such attacks (with SSL2.0 and above).
- HTTPS is marginally slower than HTTP. When large amounts of data are processing over a port, performance can degrade**.