# Encrypting the World Wide Web

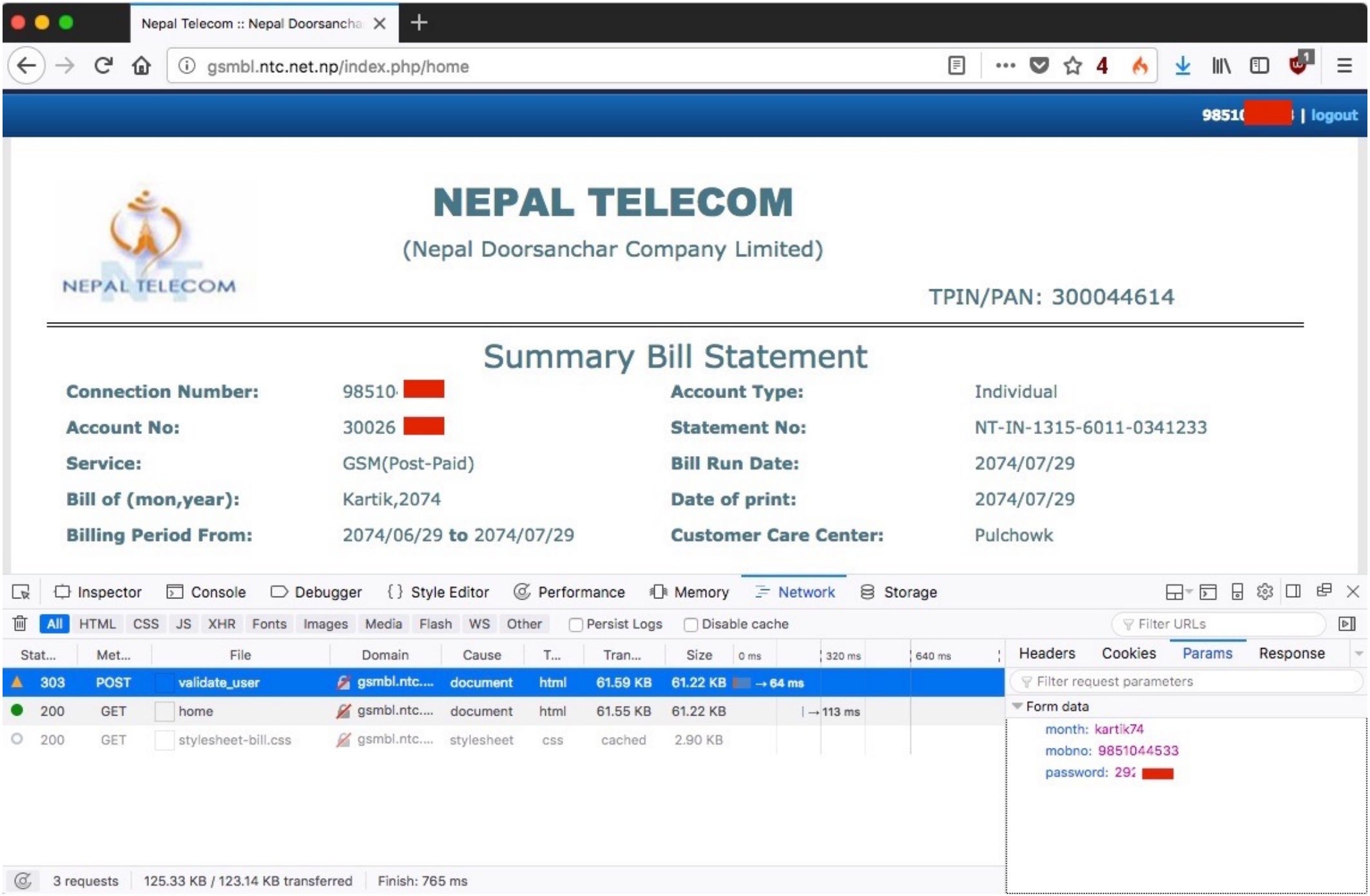
**Indiver Badal**
Mavorion Systems Pvt. Ltd.
(NPIX, NPNOG, NREN)

# Background - TLS

- Transport Layer Security (TLS)
  - Predecessor was Secure Socket Layer (SSL)
- Encryption between web server and browser
- Secures username, password and other private information transmission over the web

# Why TLS

- What happens when not TLS is used?


Nepal Telecom :: Nepal Doorsancha
gsmbl.ntc.net.np/index.php/home
98510 | logout
NEPAL TELECOM
(Nepal Doorsanchar Company Limited)
TPIN/PAN: 300044614
Summary Bill Statement
Connection Number: 98510
Account Type: Individual
Account No: 30026
Statement No: NT-IN-1315-6011-0341233
Service: GSM(Post-Paid)
Bill Run Date: 2074/07/29
Bill of (mon,year): Kartik,2074
Date of print: 2074/07/29
Billing Period From: 2074/06/29 to 2074/07/29
Customer Care Center: Pulchowk
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
All HTML CSS JS XHR Fonts Images Media Flash WS Other
Persist Logs
Disable cache
Filter URLs
Stat... Met... File Domain Cause T... Tran... Size
303 POST validate_user gsmbl.ntc.... document html 61.59 KB 61.22 KB → 64 ms
200 GET home gsmbl.ntc.... document html 61.55 KB 61.22 KB → 113 ms
200 GET stylesheet-bill.css gsmbl.ntc.... stylesheet css cached 2.90 KB
Headers Cookies Params Response
Filter request parameters
Form data
month: kartik74
mobno: 9851044533
password: 29
3 requests
125.33 KB / 123.14 KB transferred
Finish: 765 ms

# What does TLS Solve?

- Secure transmission of:
  - Login information
  - Banking data
  - Online document
  - Social network activities
- Secures online activities from surveillance by Hotspot operator or ISP

# Problem

- TLS is not still not everywhere in 2017
- Setting up TLS (without LE) is still tedious
  - Generate Private Keys & Generate CSR on your Web Server
  - Login to Certificate provider
  - Provide CSR, Make Payment, Prove ownership of domain
  - Get the certs -> Unzip -> Transfer to web-server
  - Configure the certs
- Alternatively, you let your certificate provider generate private keys for you.
- Renewal - is similarly tedious

# Let's Encrypt

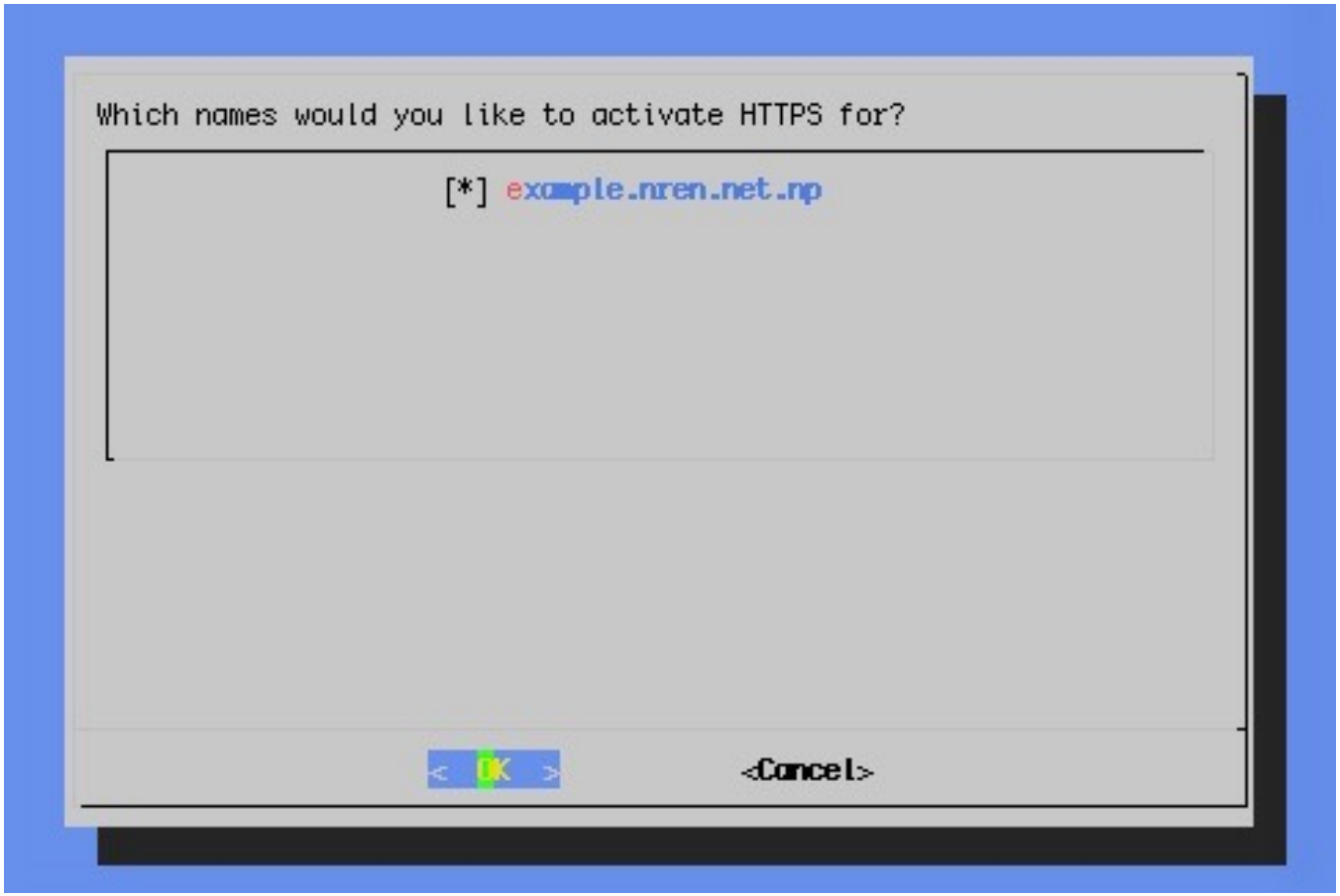
- Easily obtain and manage certificates
  - A CA that provides free X.509 certificates for TLS
  - Tools to use on web-servers to obtain and configure certificates
  - Automated domain validation
  - Tools to renew the certificates automatically

# Step-by-step 1

- Install Let's Encrypt client on your webserver
  - $ sudo apt-get install letsencrypt
  - $ sudo letsencrypt

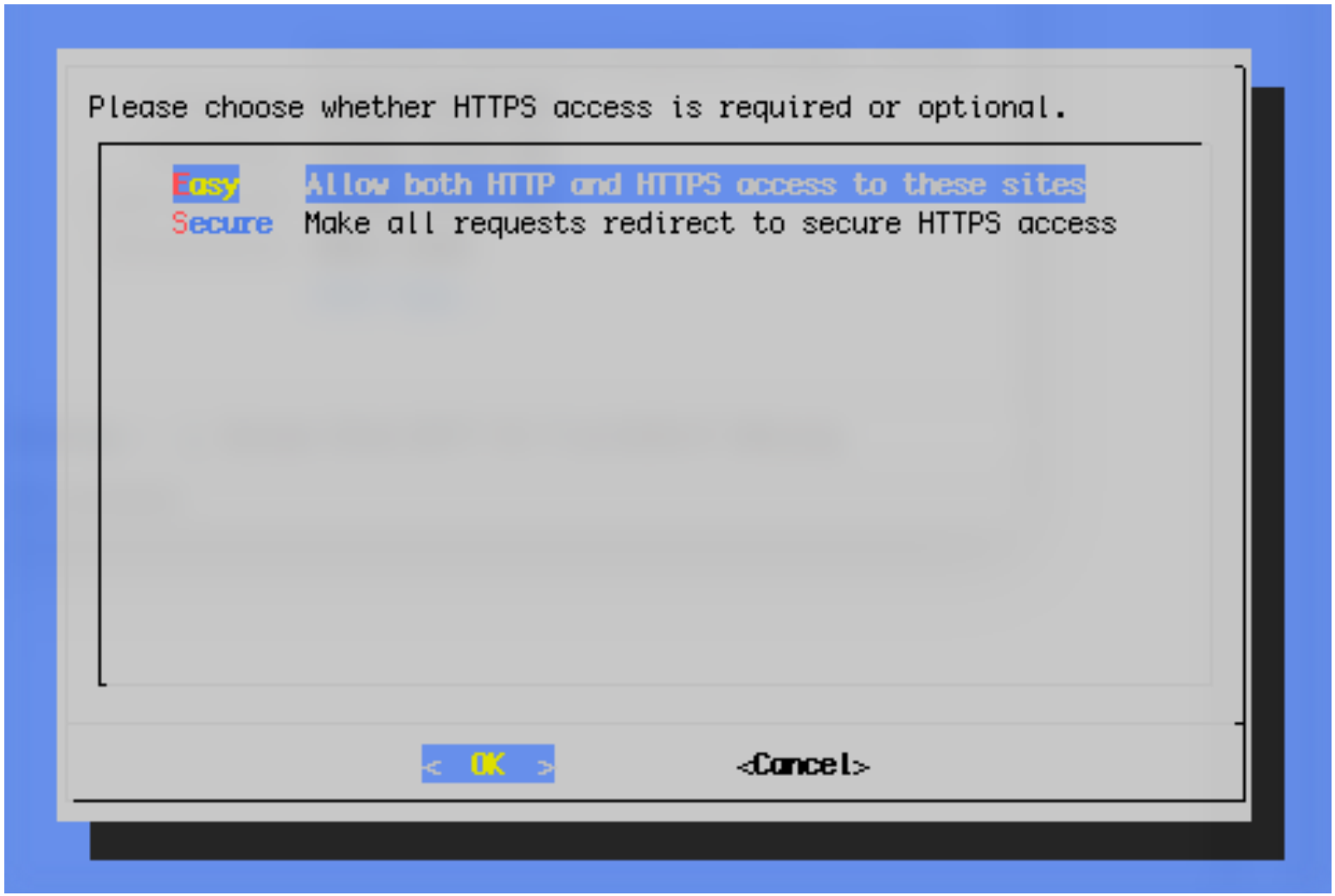
# Step-by-step 2

- Select the website
  - Follow instructions



# Step-by-step 3

- Easy vs Secure



# Let's Encrypt automates

- Generating Private Keys and CSR
- Communicating with CA
  - Provide CSR
  - Prove ownership of domain
  - Obtain the certificates
- Configures certificates and web server (including virtual-host settings), reloads web server
- TLS now ready

# Certificate Renewal

- $ sudo crontab -e
- Enter the following line at the end

```
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
30 11 * * 1 /usr/bin/letsencrypt renew >> /var/log/letsencrypt.log
```

- If there are any certificates close to expiry, they are renewed automatically

# Fully Automated

- Setup once and it is fully automated
  - Single tool to manage several tedious steps
  - Same tool for validation
- Email alerts if a certificate is close to expiry
- Scriptable

# Summary

- Start encrypting all transmissions
- LE makes certificates very easy to obtain, implement and renew
- Probably the easiest
  - Some control panel solutions are now easier as well

# Thanks

- Questions?

- indiver@mavorion.com
- Subscribe to **npnog** mailing list
  - Go to URL: http://lists.npnog.org