ezTCP Application Note

# SSL (Secure Socket Layer)

Version 1.3

Sollae Systems Co., Ltd.

http://www.ezTCP.com

# Contents

# 1 Introduction

## 1.1 SSL (Secure Socket Layer)

The Secure Socket Layer (SSL), developed by Netscape Company, was originally designed for secure electronic commerce and other Web transactions on the Internet. It was standardized as TLS (Transport Layer Security) by IETF (Internet Engineering Task Force) developing and promoting Internet standards. The latest version of SSL and TLS is the 3.0 and 1.0 respectively.

## 1.2 SSL with the ezTCP

The ezTCP guarantees the security of communications on the Internet by supporting SSL 3.0 / TLS 1.0. This application note introduces how to use “SSL” feature for CSE-M32, CSE-H20, CSE-H21, CSE-M73 and CSE-H25.

# 2 Setting

## 2.1 Limitations

- Cannot use SSL feature in "U2S – UDP" Communication Mode

- User cannot use the following features
  SSH and Telnet COM Port Control(RFC2217)

- Restrictions while using SSL feature on each product

  <CSE-M32, CSE-H20, CSE-H21>
  Maximum baud rate of serial port is the 115,200bps / COM2 serial port is disabled

  <CSE-M73, CSE-H25>
  Maximum baud rate of serial port is the 115,200bps / "Multi Monitoring" feature is disabled

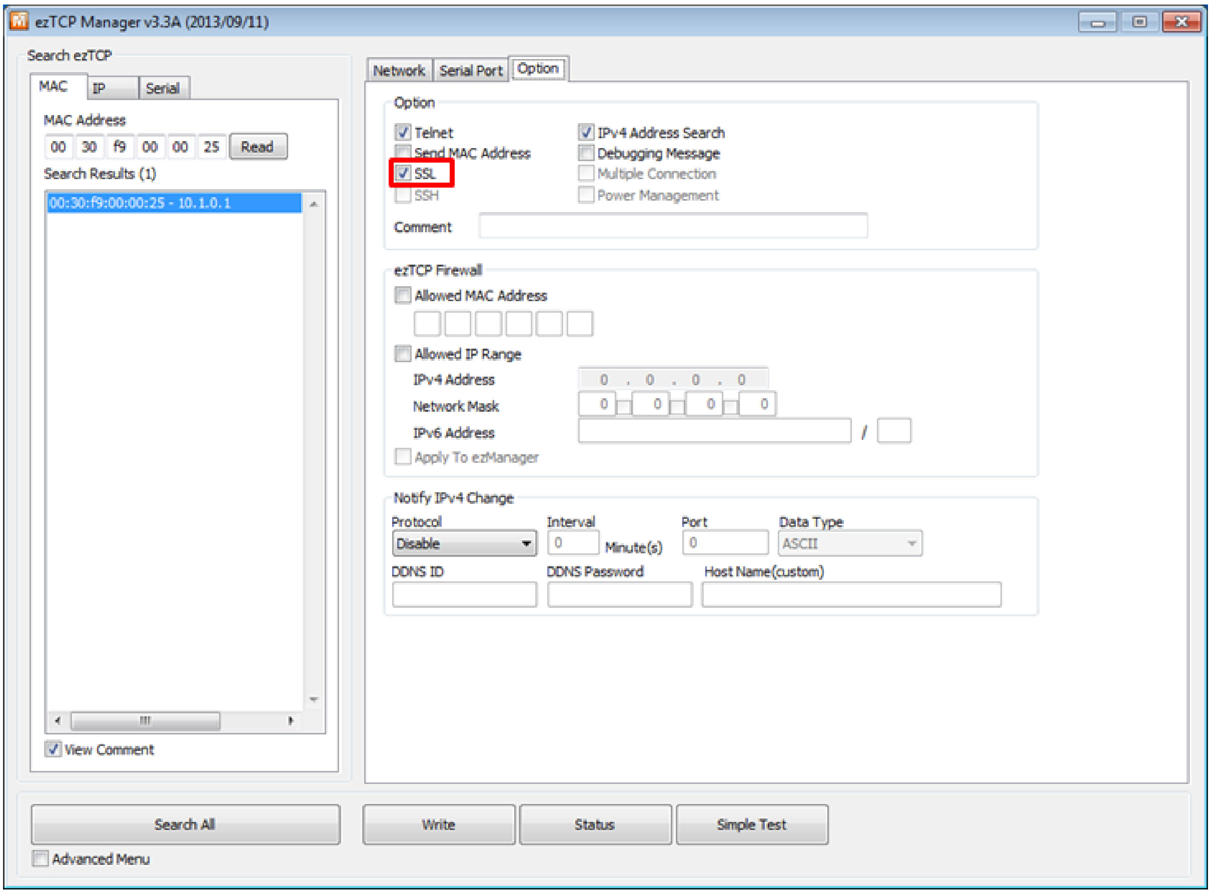
## 2.2 Set up "SSL" feature

### 2.2.1 Overview

SSL function can be used TCP server as well as TCP client mode. In the case of TCP client mode, just check [SSL] in "Option" tab of ezManager. Then you can make SSL connection. On the other hand, you should connect on Telnet and make certification when using TCP server mode.

### 2.2.2 Setting with ezManager

Check [SSL] in “OPTION” tab of ezManager.



MAC Address: 00 30 f9 00 00 25
Search Results (1): 00:30:f9:00:00:25 - 10.1.0.1
☑ View Comment
□ Advanced Menu

Option
☑ Telnet
□ Send MAC Address
☑ SSL
□ SSH
☑ IPv4 Address Search
□ Debugging Message
□ Multiple Connection
□ Power Management
Comment

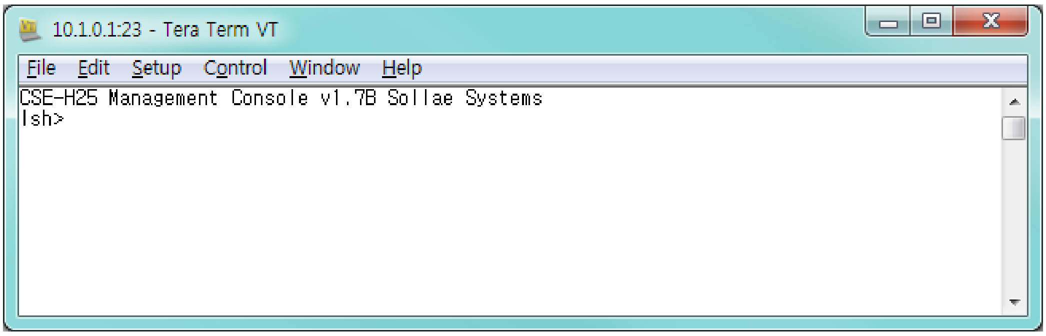
ezTCP Firewall
□ Allowed MAC Address
□ Allowed IP Range
IPv4 Address: 0 . 0 . 0 . 0
Network Mask: 0 0 0 0
IPv6 Address: /
□ Apply To ezManager

Notify IPv4 Change
Protocol: Disable
Interval: 0 Minute(s)
Port: 0
Data Type: ASCII
DDNS ID
DDNS Password
Host Name(custom)

Figure 2-1 Setting “SSL” option

### 2.2.3 SSL certificate generation

- Connect to TELNET console by a TELNET client.



```
CSE-H25 Management Console v1.7B Sollae Systems
lsh>
```

Figure 2-2 connect to TELNET console

☞ ***Entering a password is required if you set a password to your product. Starting with firmware version 2.0A, you need to enter "sollae" without setting a password.***

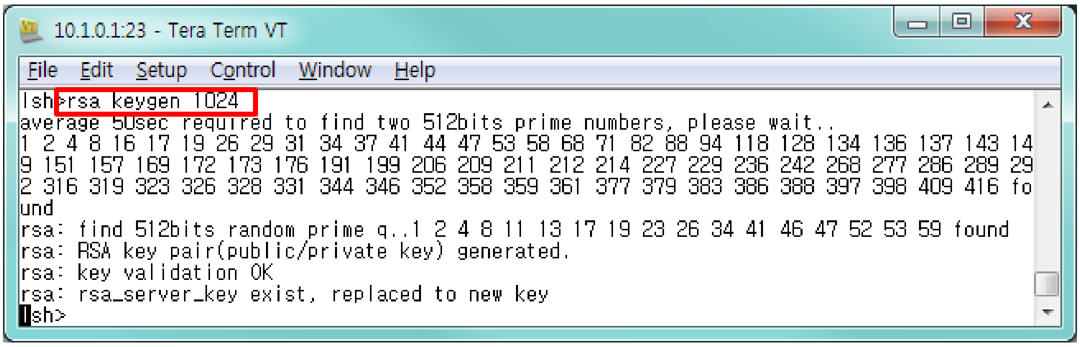
- The following is the telnet console command list

| Item | Command | Descriptions |
|---|---|---|
| RSA KEY | rsa keygen <key length> | supporting KEY length 512/768/1024 |
| | rsa key | Confirm generated RSA KEY |
| | rsa test | Check RSA KEY is correctly generated |
| Certificate | cert new | Generate certificate from RSA KEY |
| | cert view | Confirm generated certificate |
| Save | ssl save aa55cc33 | Save the configuration of SSL related parameter |

Table 2-1 Telnet commands for setting SSL option

- RSA KEY generation

Generate RSA KEY first for certificate generation. The ezTCP supports 512, 768 and 1024 bytes KEY length. In accordance with the KEY length, KEY generation may take a number of minutes. Longer KEY length provides more secure communications and takes longer time for KEY generation. For example, 1024-bit KEY length may take about 1 minute on average. The command form is "rsa keygen <key length>" as shown below.



```
lsh>rsa keygen 1024
average 50sec required to find two 512bits prime numbers, please wait..
1 2 4 8 16 17 19 26 29 31 34 37 41 44 47 53 58 68 71 82 88 94 118 128 134 136 137 143 14
9 151 157 169 172 173 176 191 199 206 209 211 212 214 227 229 236 242 268 277 286 289 29
2 316 319 323 326 328 331 344 346 352 358 359 361 377 379 383 386 388 397 398 409 416 fo
und
rsa: find 512bits random prime q..1 2 4 8 11 13 17 19 23 26 34 41 46 47 52 53 59 found
rsa: RSA key pair(public/private key) generated.
rsa: key validation OK
rsa: rsa_server_key exist, replaced to new key
lsh>
```

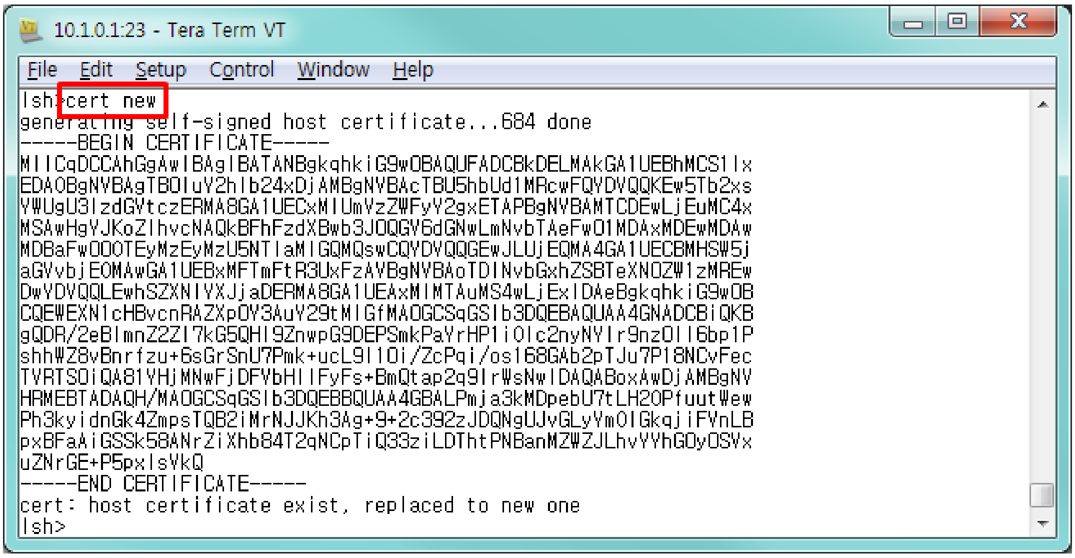
Figure 2-3 RSA KEY generation

This RSA KEY can check if it is correctly generated by "rsa test" command. The present generated RSA KEY can be confirmed by "rsa key" command.

☞ ***When you generate a new RSK KEY, the old one is replaced with the new one.***

- Digital certificate generation

  If RSA KEY is generated successfully, a certificate can be generated by "cert new" command.


10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help

```
lsh>cert new
generating self-signed host certificate...684 done
-----BEGIN CERTIFICATE-----
MIICqDCCAhGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBkDELMAkGA1UEBhMCS1Ix
EDAOBgNVBAgTB0luY2hlb24xDjAMBgNVBAcTBU5hbUd1MRcwFQYDVQQKEw5Tb2xs
YWUgU3lzdGVtczERMA8GA1UECxMIUmVzZWFyY2gxETAPBgNVBAMTCDEwLjEuMC4x
MSAwHgYJKoZIhvcNAQkBFhFzdXBwb3J0QGV6dGNwLmNvbTAeFw01MDAxMDEwMDAw
MDBaFw00OTEyMzEyMzU5NTlaMIGQMQswCQYDVQQGEwJLUjEQMA4GA1UECBMHSW5j
aGVvbjEOMAwGA1UEBxMFTmFtR3UxFzAVBgNVBAoTDlNvbGxhZSBTeXN0ZW1zMREw
DwYDVQQLEwhSZXNlYXJjaDERMA8GA1UEAxMIMTAuMS4wLjExIDAeBgkqhkiG9w0B
CQEWEXN1cHBvcnRAZXp0Y3AuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDR/2eBlmnZ2Zl7kG5QHl9ZnwpG9DEPSmkPaYrHP1iOlc2nyNYlr9nzOll6bp1P
shhWZ8vBnrfzu+6sGrSnU7Pmk+ucL9l10i/ZcPqi/os168GAb2pTJu7P18NCvFec
TVRTSOiQA81YHjMNwFjDFVbHllFyFs+BmQtap2q9lrWsNwIDAQABoxAwDjAMBgNV
HRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4GBALPmja3kMDpebU7tLH2OPfuutWew
Ph3kyidnGk4ZmpsTQB2iMrNJJKh3Ag+9+2c392zJDQNgUJvGLyYm0lGkqjiFVnLB
pxBFaAiGSSk58ANrZiXhb84T2qNCpTiQ33ziLDThtPNBanMZWZJLhvYYhGOyOSVx
uZNrGE+P5pxlsVkQ
-----END CERTIFICATE-----
cert: host certificate exist, replaced to new one
lsh>
```

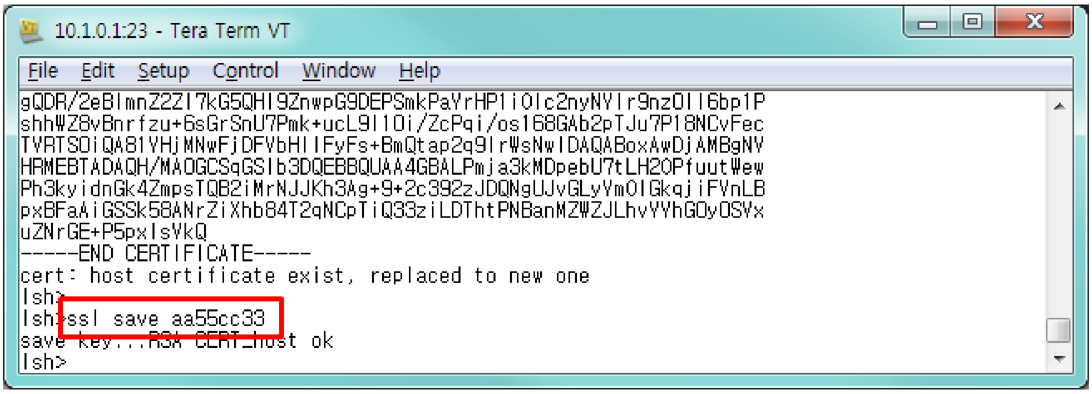
Figure 2-4 Certificate generation

Unlike a TCP client, this step is required to TCP server. A new digital certificate should be generated whenever a local IP address of ezTCP is changed, because it contains the IP address information.

☞ ***When you generate a new certificate, the old one is replaced with the new one.***

- Save the configuration

  The RSA KEY and the digital certificate have to be saved to the flash memory of ezTCP for using SSL feature. The command form is "ssl save aa55cc33".


10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help

```
gQDR/2eBlmnZ2Zl7kG5QHl9ZnwpG9DEPSmkPaYrHP1iOlc2nyNYlr9nzOll6bp1P
shhWZ8vBnrfzu+6sGrSnU7Pmk+ucL9l10i/ZcPqi/os168GAb2pTJu7P18NCvFec
TVRTSOiQA81YHjMNwFjDFVbHllFyFs+BmQtap2q9lrWsNwIDAQABoxAwDjAMBgNV
HRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4GBALPmja3kMDpebU7tLH2OPfuutWew
Ph3kyidnGk4ZmpsTQB2iMrNJJKh3Ag+9+2c392zJDQNgUJvGLyYm0lGkqjiFVnLB
pxBFaAiGSSk58ANrZiXhb84T2qNCpTiQ33ziLDThtPNBanMZWZJLhvYYhGOyOSVx
uZNrGE+P5pxlsVkQ
-----END CERTIFICATE-----
cert: host certificate exist, replaced to new one
lsh>
lsh>ssl save aa55cc33
save key...RSA CERT_host ok
lsh>
```

Figure 2-5 Save SSL configuration

# 3 Examples of use

## 3.1 Overview

### 3.1.1 TCP connection type

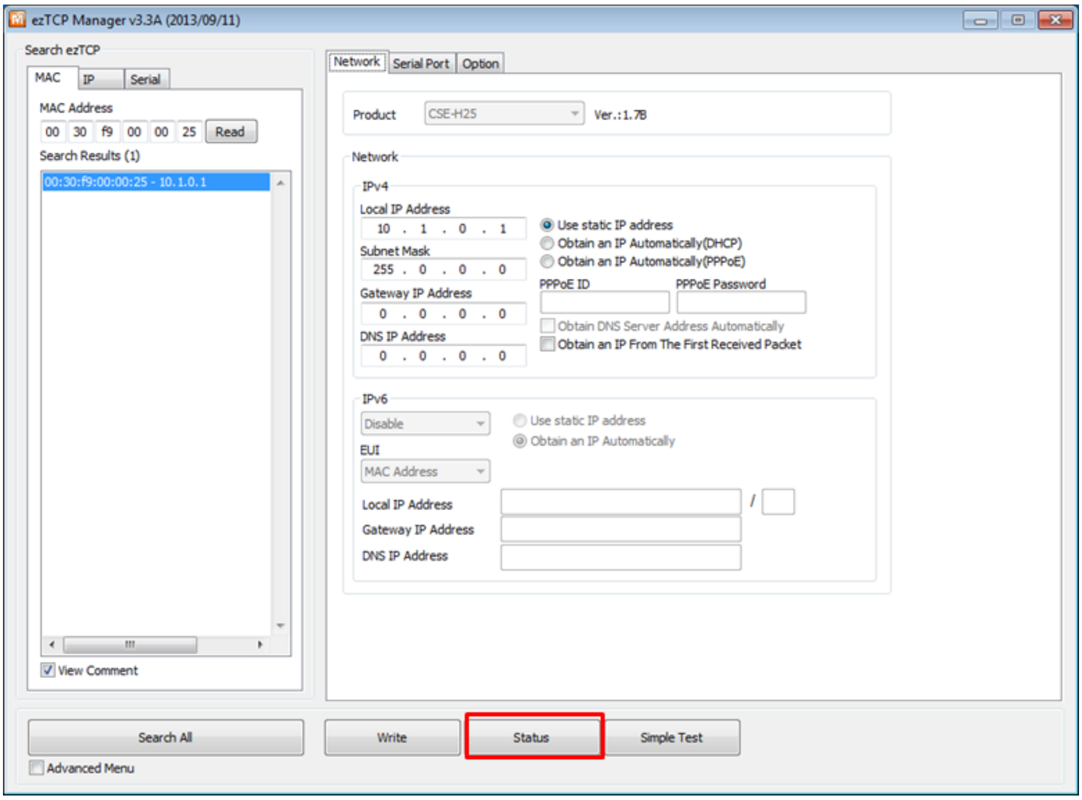
SSL requires TCP and communication mode for TCP is as follows.

- TCP Server
  T2S – TCP Server mode
  TCP passive connection by “ata” command in ATC – AT Command mode
- TCP Client
  COD – TCP Client mode
  TCP active connection by “atd(t)” command in ATC – AT Command mode

## 3.2 TCP Server

### 3.2.1 Setting Confirmation with ezManager

Click the [Status] button of ezManager.



MAC Address: 00 30 f9 00 00 25
Search Results (1)
00:30:f9:00:00:25 - 10.1.0.1
☑ View Comment
□ Advanced Menu

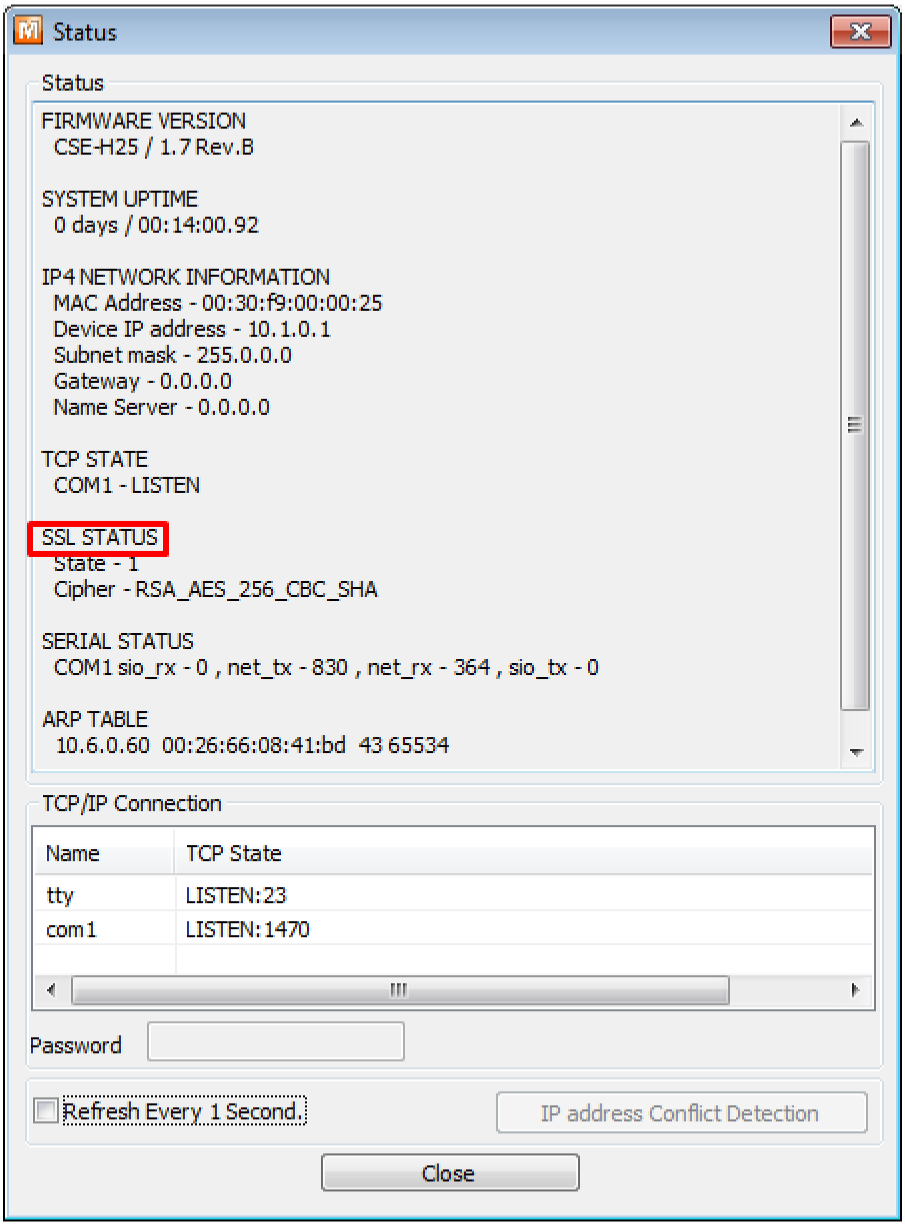
Product: CSE-H25 Ver.:1.7B

Network

IPv4
Local IP Address: 10 . 1 . 0 . 1
Subnet Mask: 255 . 0 . 0 . 0
Gateway IP Address: 0 . 0 . 0 . 0
DNS IP Address: 0 . 0 . 0 . 0
● Use static IP address
○ Obtain an IP Automatically(DHCP)
○ Obtain an IP Automatically(PPPoE)
PPPoE ID
PPPoE Password
□ Obtain DNS Server Address Automatically
□ Obtain an IP From The First Received Packet

IPv6
Disable
○ Use static IP address
● Obtain an IP Automatically
EUI
MAC Address
Local IP Address /
Gateway IP Address
DNS IP Address

Figure 3-1 ezManager



```
FIRMWARE VERSION
  CSE-H25 / 1.7 Rev.B

SYSTEM UPTIME
  0 days / 00:14:00.92

IP4 NETWORK INFORMATION
  MAC Address - 00:30:f9:00:00:25
  Device IP address - 10.1.0.1
  Subnet mask - 255.0.0.0
  Gateway - 0.0.0.0
  Name Server - 0.0.0.0

TCP STATE
  COM1 - LISTEN

SSL STATUS
  State - 1
  Cipher - RSA_AES_256_CBC_SHA

SERIAL STATUS
  COM1 sio_rx - 0 , net_tx - 830 , net_rx - 364 , sio_tx - 0

ARP TABLE
  10.6.0.60  00:26:66:08:41:bd  43 65534
```

TCP/IP Connection

| Name | TCP State |
|---|---|
| tty | LISTEN:23 |
| com1 | LISTEN:1470 |

Password:

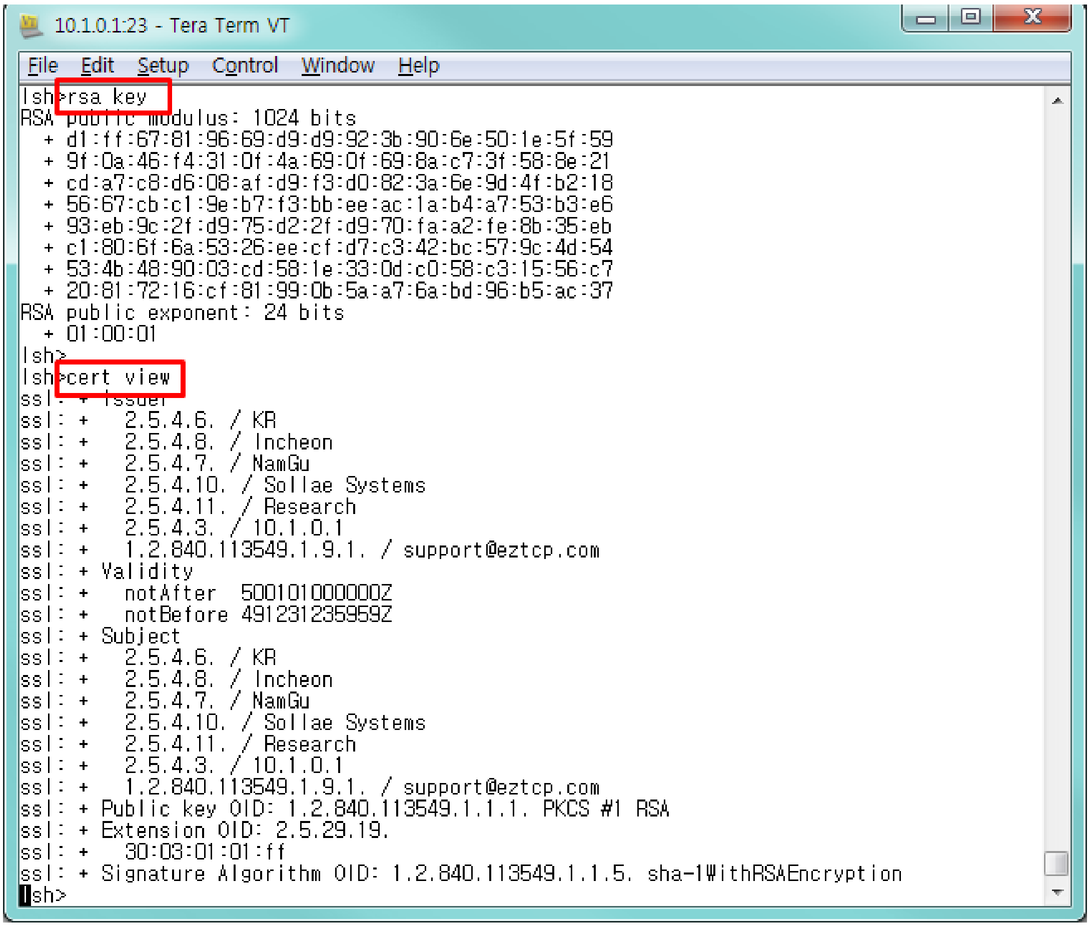
□ Refresh Every 1 Second.

Figure 3-2 ezManager [Status]

Check if there is “SSL STATUS” as shown above.

### 3.2.2 Setting Confirmation with Telnet console

After logging in telnet console of ezTCP, check both RSA KEY and digital certificate. The related command is "rsa key" and "cert view". Especially, check if the current IP address of ezTCP is the same with the IP address information of the digital certificate.


10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help

```
lsh>rsa key
RSA public modulus: 1024 bits
  + d1:ff:67:81:96:69:d9:d9:92:3b:90:6e:50:1e:5f:59
  + 9f:0a:46:f4:31:0f:4a:69:0f:69:8a:c7:3f:58:8e:21
  + cd:a7:c8:d6:08:af:d9:f3:d0:82:3a:6e:9d:4f:b2:18
  + 56:67:cb:c1:9e:b7:f3:bb:ee:ac:1a:b4:a7:53:b3:e6
  + 93:eb:9c:2f:d9:75:d2:2f:d9:70:fa:a2:fe:8b:35:eb
  + c1:80:6f:6a:53:26:ee:cf:d7:c3:42:bc:57:9c:4d:54
  + 53:4b:48:90:03:cd:58:1e:33:0d:c0:58:c3:15:56:c7
  + 20:81:72:16:cf:81:99:0b:5a:a7:6a:bd:96:b5:ac:37
RSA public exponent: 24 bits
  + 01:00:01
lsh>
lsh>cert view
ssl: + Issuer
ssl: +   2.5.4.6. / KR
ssl: +   2.5.4.8. / Incheon
ssl: +   2.5.4.7. / NamGu
ssl: +   2.5.4.10. / Sollae Systems
ssl: +   2.5.4.11. / Research
ssl: +   2.5.4.3. / 10.1.0.1
ssl: +   1.2.840.113549.1.9.1. / support@eztcp.com
ssl: + Validity
ssl: +   notAfter  500101000000Z
ssl: +   notBefore 491231235959Z
ssl: + Subject
ssl: +   2.5.4.6. / KR
ssl: +   2.5.4.8. / Incheon
ssl: +   2.5.4.7. / NamGu
ssl: +   2.5.4.10. / Sollae Systems
ssl: +   2.5.4.11. / Research
ssl: +   2.5.4.3. / 10.1.0.1
ssl: +   1.2.840.113549.1.9.1. / support@eztcp.com
ssl: + Public key OID: 1.2.840.113549.1.1.1. PKCS #1 RSA
ssl: + Extension OID: 2.5.29.19.
ssl: +   30:03:01:01:ff
ssl: + Signature Algorithm OID: 1.2.840.113549.1.1.5. sha-1WithRSAEncryption
lsh>
```

Figure 3-3 confirm RSA KEY and Certificate

### 3.2.3 Connecting to ezTCP

To communicate with the ezTCP whose SSL feature is enabled, a remote host must support SSL. Confirm SSL feature by using ezVSP supporting SSL.

- Checking network environment

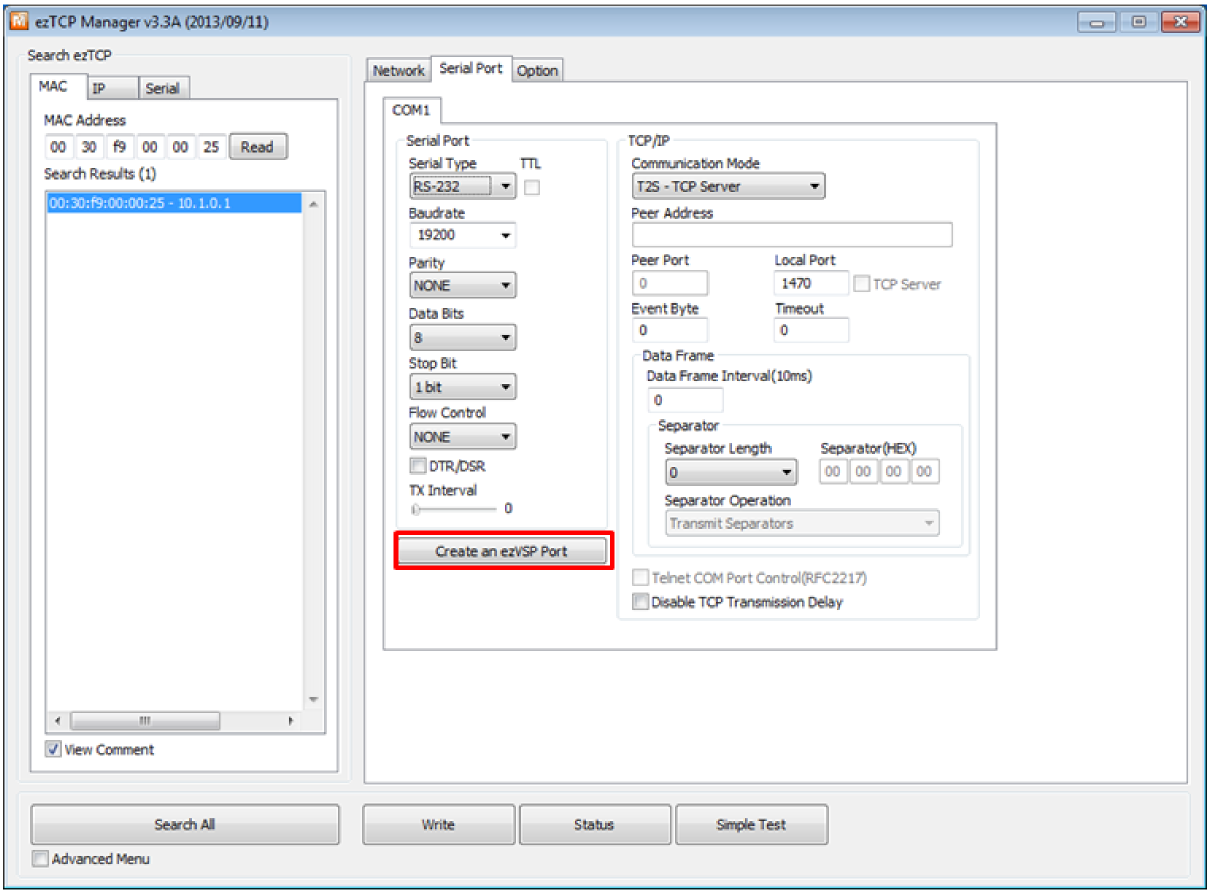
  Configure network parameters such as IP addresses to make sure that PC can access to ezTCP. Refer to the example which uses factory default values.

| Division | ezTCP | PC |
|---|---|---|
| IP Address | 10.1.0.1 | 10.1.0.2 |
| Subnet Mask | 255.0.0.0 | 255.0.0.0 |
| Local Port | 1470 | - |

Table 3-1 network parameters

- Setting ezVSP

  Click the [Create an ezVSP Port] button of ezManager.



ezTCP Manager v3.3A (2013/09/11)

Search ezTCP: MAC Address 00 30 f9 00 00 25

Search Results (1): 00:30:f9:00:00:25 - 10.1.0.1

☑ View Comment

COM1 – Serial Port

Serial Type: RS-232 □ TTL

Baudrate: 19200

Parity: NONE

Data Bits: 8

Stop Bit: 1 bit

Flow Control: NONE

□ DTR/DSR

TX Interval: 0

TCP/IP

Communication Mode: T2S - TCP Server

Peer Address:

Peer Port: 0

Local Port: 1470 □ TCP Server

Event Byte: 0

Timeout: 0

Data Frame Interval(10ms): 0

Separator Length: 0

Separator(HEX): 00 00 00 00

Separator Operation: Transmit Separators

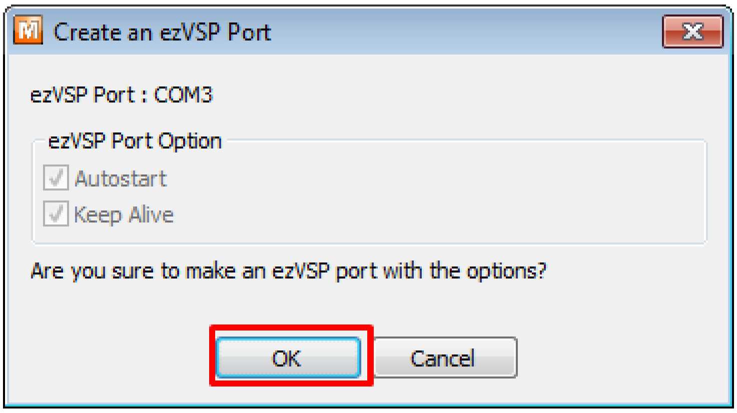
□ Telnet COM Port Control(RFC2217)

□ Disable TCP Transmission Delay

□ Advanced Menu

Figure 3-4 create an ezVSP port(1)

Click the [OK] button.



Create an ezVSP Port

ezVSP Port : COM3

ezVSP Port Option

☑ Autostart

☑ Keep Alive

Are you sure to make an ezVSP port with the options?

Figure 3-5 create an ezVSP port(2)

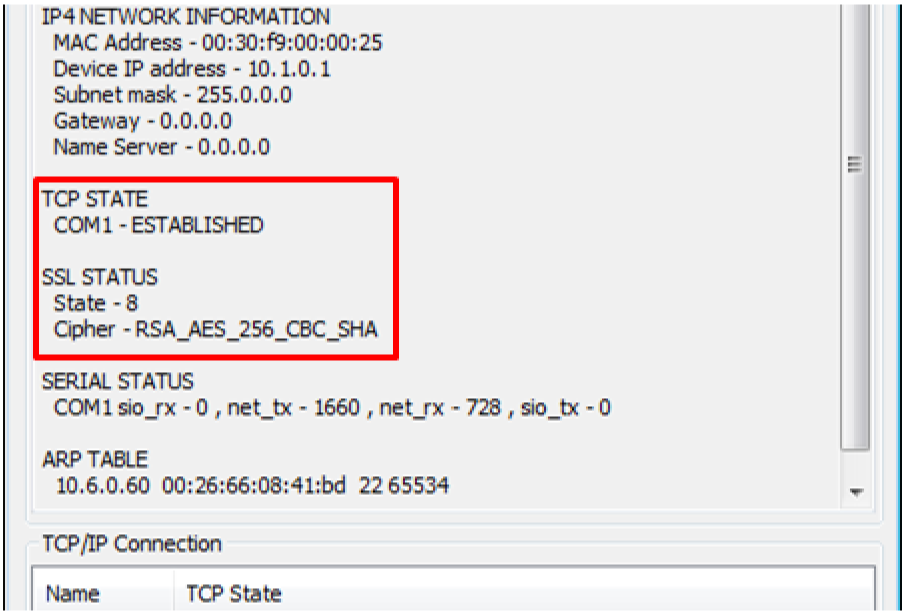
Refer to ezVSP user manual for installing ezVSP program and detailed information.

☞ ***ezVSP, which is Virtual Com Port Redirector, offers our customer to convert TCP/IP data to serial like ezTCP. Please refer to the manual for details about the program.***

- Confirm TCP connection

  Once virtual COM port is started, SSL connection is established between ezTCP and the VSP. Check if the connection is fine by [Status] button on ezManager.

  You can find "COM1 - ESTABLISHED" in the "TCP STATE" and [State - 7(or 8)] and [Cipher - RSA_AES_256_CBC_SHA] in the "SSL STATUS", if the connection is fine.



```
IP4 NETWORK INFORMATION
  MAC Address - 00:30:f9:00:00:25
  Device IP address - 10.1.0.1
  Subnet mask - 255.0.0.0
  Gateway - 0.0.0.0
  Name Server - 0.0.0.0

TCP STATE
  COM1 - ESTABLISHED

SSL STATUS
  State - 8
  Cipher - RSA_AES_256_CBC_SHA

SERIAL STATUS
  COM1 sio_rx - 0 , net_tx - 1660 , net_rx - 728 , sio_tx - 0

ARP TABLE
  10.6.0.60  00:26:66:08:41:bd  22 65534
```

TCP/IP Connection

| Name | TCP State |
|---|---|

Figure 3-6 confirm TCP connection of SSL feature

## 3.3 TCP Client mode

When your ezTCP is set to TCP client mode, enabling [SSL] option is only required to make SSL connection. In this case, TCP server should available on SSL connection, too. To confirm current SSL connection, use the [Status] button of ezManager.

# 4 Revision History

| Date | Version | Comments | Author |
|---|---|---|---|
| 2008.09.16 | 1.0 | ○ Initial Release | - |
| 2009.06.11 | 1.1 | ○ Modify images and terms<br>○ Add product CSE-H25 | - |
| 2015.02.06 | 1.2 | ○ Update figures<br>○ Correct some errors and expressions | Roy LEE |
| 2016.04.07 | 1.3 | ○ Add an explanation about TELNET login | Roy LEE |