Application Note

SSL (Secure Socket Layer)

Version 1.1

2009-06-11

Sollae Systems Co., Ltd. http://www.sollae.co.kr

Contents

1 Introduction

1.1 Terminology

- "ezTCP"
  ezTCP is the brand name of Sollae's products. It provides Internet connection to common serial communication devices.
- "host"
  A computer (or some network device – e.g. ezTCP) connected to the Internet (or local private network)
- "TCP/IP"
  TCP/IP is the set of communication protocols used for the Internet and private networks.

1.2 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) develops and promotes Internet standards. The latest version of SSL and TLS is the 3.0 and 1.0 respectively.

1.3 Communication Mode

The ezTCP has four "Communication Mode" for TCP/IP communication like T2S – TCP Server, ATC – AT Command, COD – TCP Client and U2S – UDP. Each Mode operates as below.

Communication Mode	TCP/IP
T2S – TCP Server	TCP (Server only)
ATC – AT Command	TCP (both Server and Client)
COD – TCP Client	TCP (Client only)
U2S – UDP	UDP

Table 1-1 Communication Mode of the ezTCP

1.4 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 product 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 below features
  SSH, Telnet COM Port Control(RFC2217)

- Restrictions while using SSL feature by each products
  <All ezTCPs>
  – Maximum baud rate of serial port is the 115,200bps

  <CSE-M32, CSE-H20, CSE-H21>
  – COM2 serial port is disabled

  <CSE-M73>
  – "Multi Monitoring" feature is disabled

2.2 Set up "SSL" feature

2.2.1 Confirm before Setting

The IP address and Port number have to be configured appropriately to the environment with ezTCP. But, to understand simply set these parameters as shown below – factory default setting.

	PC	ezTCP
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0

2.2.2 Setting with ezManager

Set [SSL] checkbox in "OPTION" tab of ezManger.

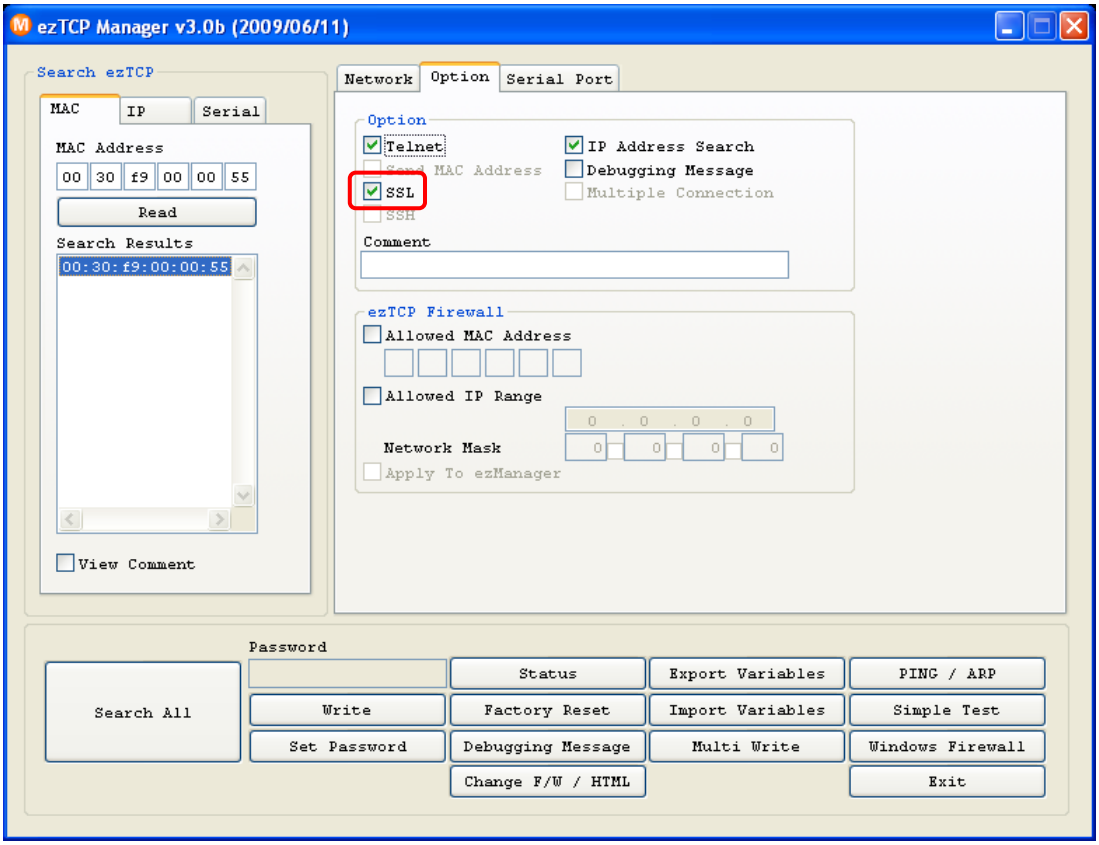

Figure 2-1 Setting "SSL" option

2.2.3 SSL certificate generation

- The below is the telnet console command lists

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 Command for setting SSL option

- Log in the telnet console of the ezTCP.

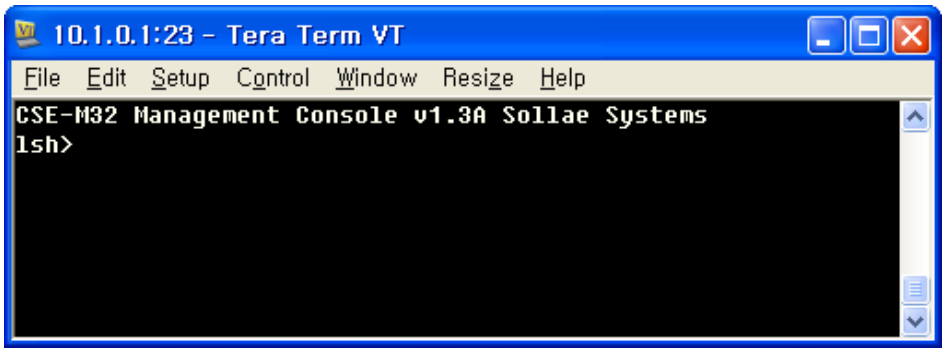

Figure 2-2 Log on telnet console

- 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.

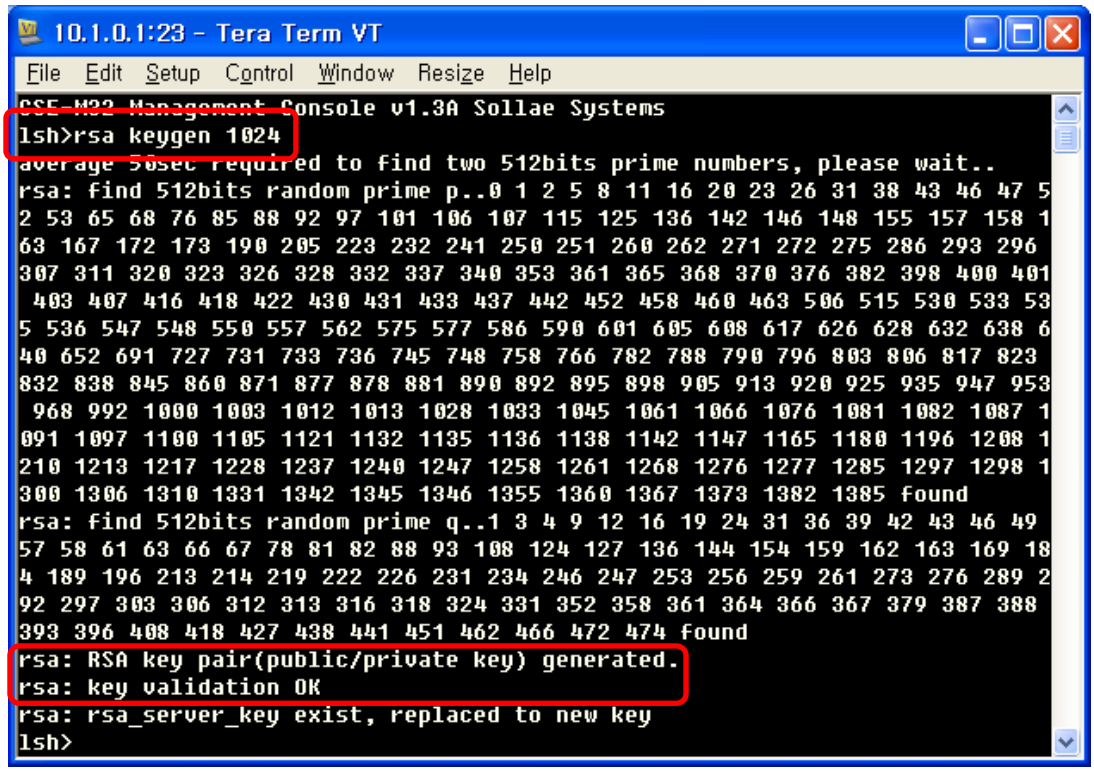

Figure 2-3 RSA KEY generation

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

- Digital certificate generation

If RSA KEY is generated successfully, generate certificate by "cert new" command. There are two types of certificates, "Public certificates and Private certificates. The former is guaranteed the validity by the public internet "Certificate Authority (CA)", the latter is guaranteed the validity by the own local "CA", for example, ezTCP itself. Because the certificate of ezTCP has its IP address information, generate the new digital certificate in each time if the IP address of ezTCP is changed.

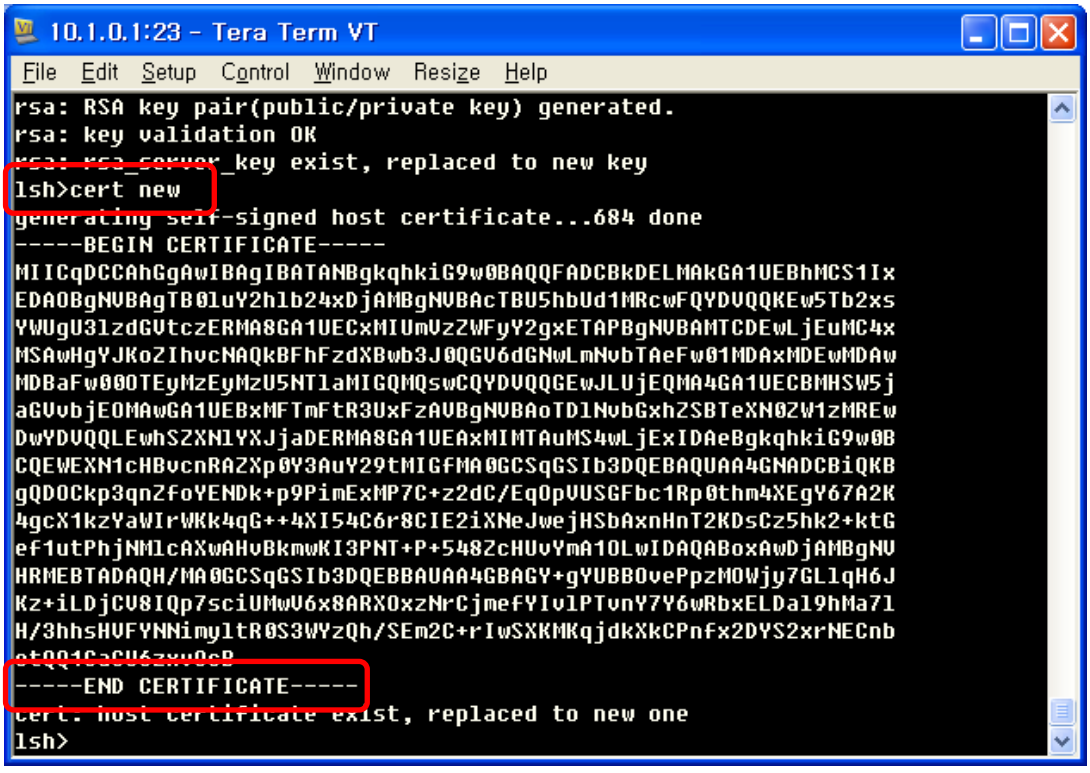

Figure 2-4 Certificate generation

- Save the configuration

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

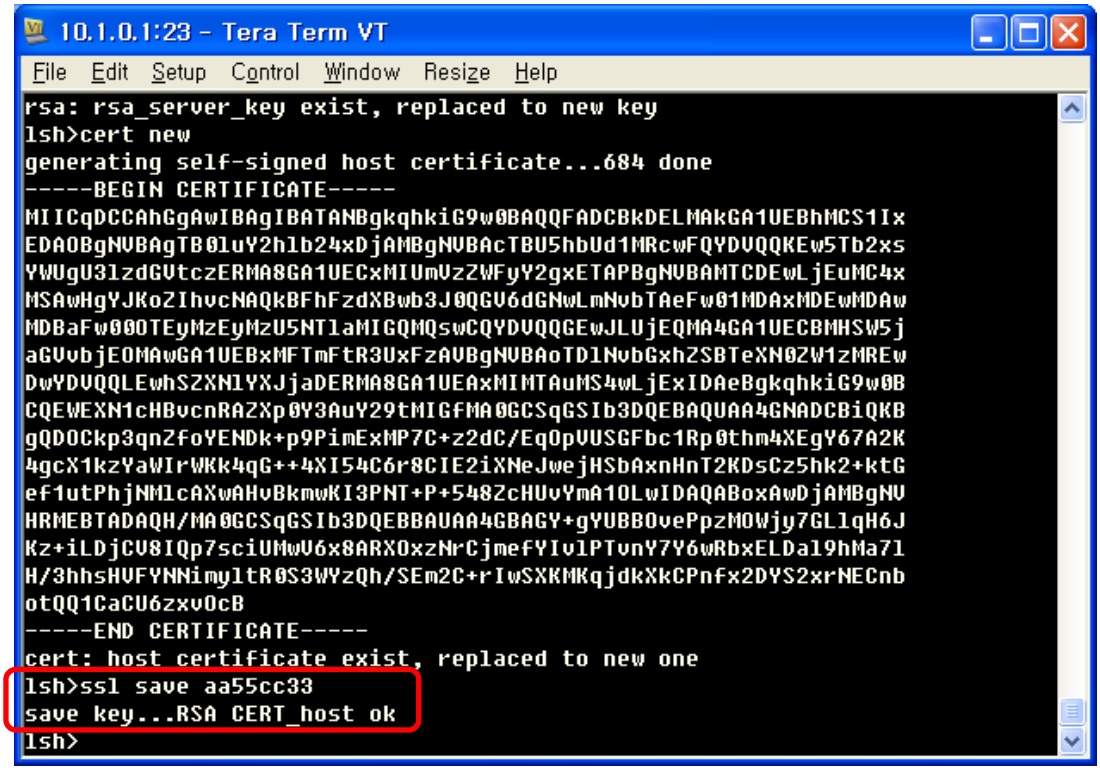

Figure 2-5 Save SSL configuration

3 Example of use

SSL requires TCP and communication mode for TCP is like below.

- TCP Server
  T2S – TCP Server mode
  TCP passive connection by "ata" command in ATC – AT Command mode

- TCP Client
  COD(2) – TCP Client mode
  TCP active connection by "atd(t)" command in ATC – AT Command mode

3.1 TCP Server

3.1.1 Confirm setting with ezManager

Click the [Status] button of ezManger.

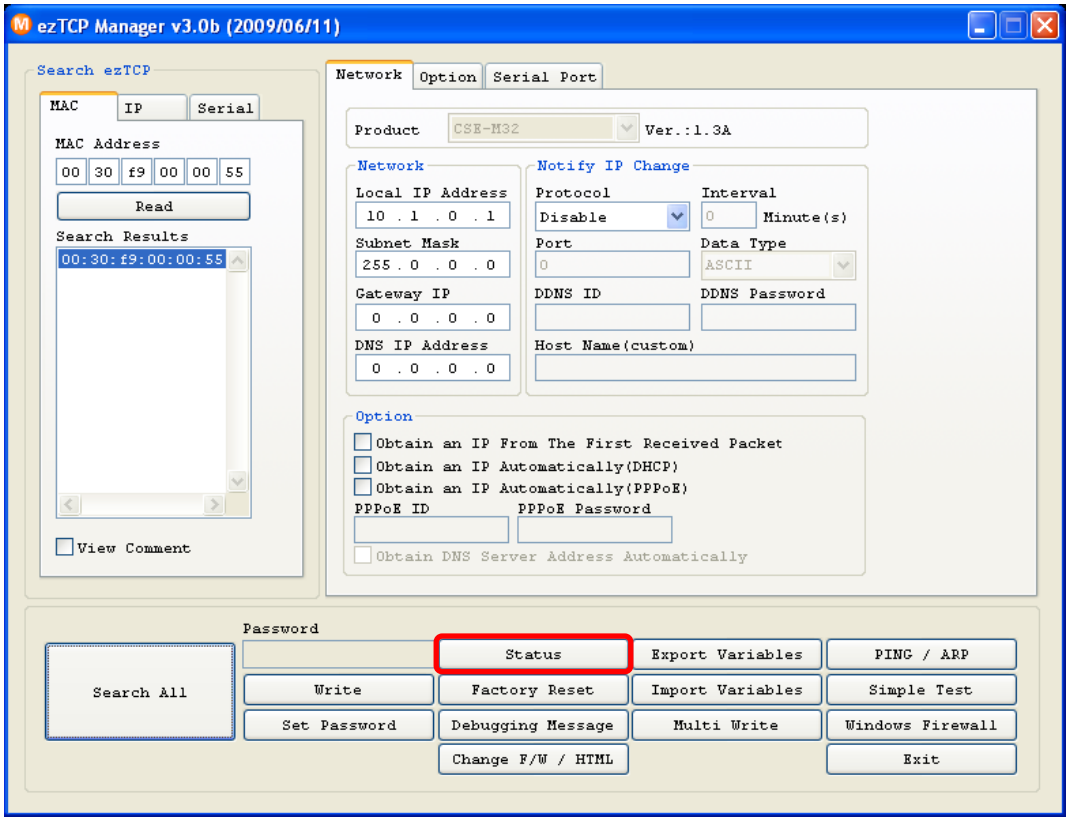

Figure 3-1 ezManager

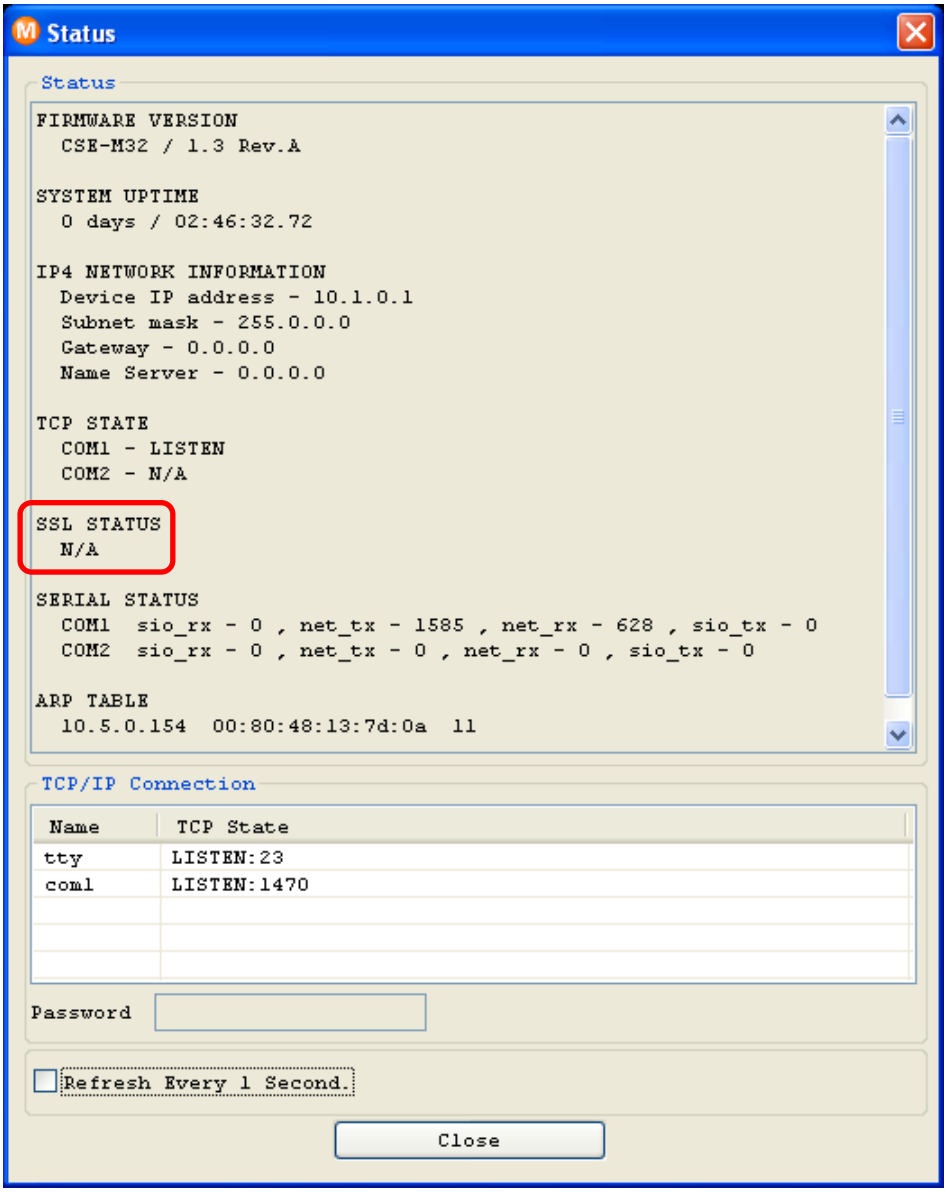

Figure 3-2 ezManager [Status]

Check if there is "SSL STATUS" as shown above.

3.1.2 Confirm setting with telnet console

After log in telnet console of ezTCP, check RSA KEY and the digital certificate. The related command is "rsa key" and "cert new". At this time, check if it is same the real IP address of ezTCP and the IP address information of the digital certificate.

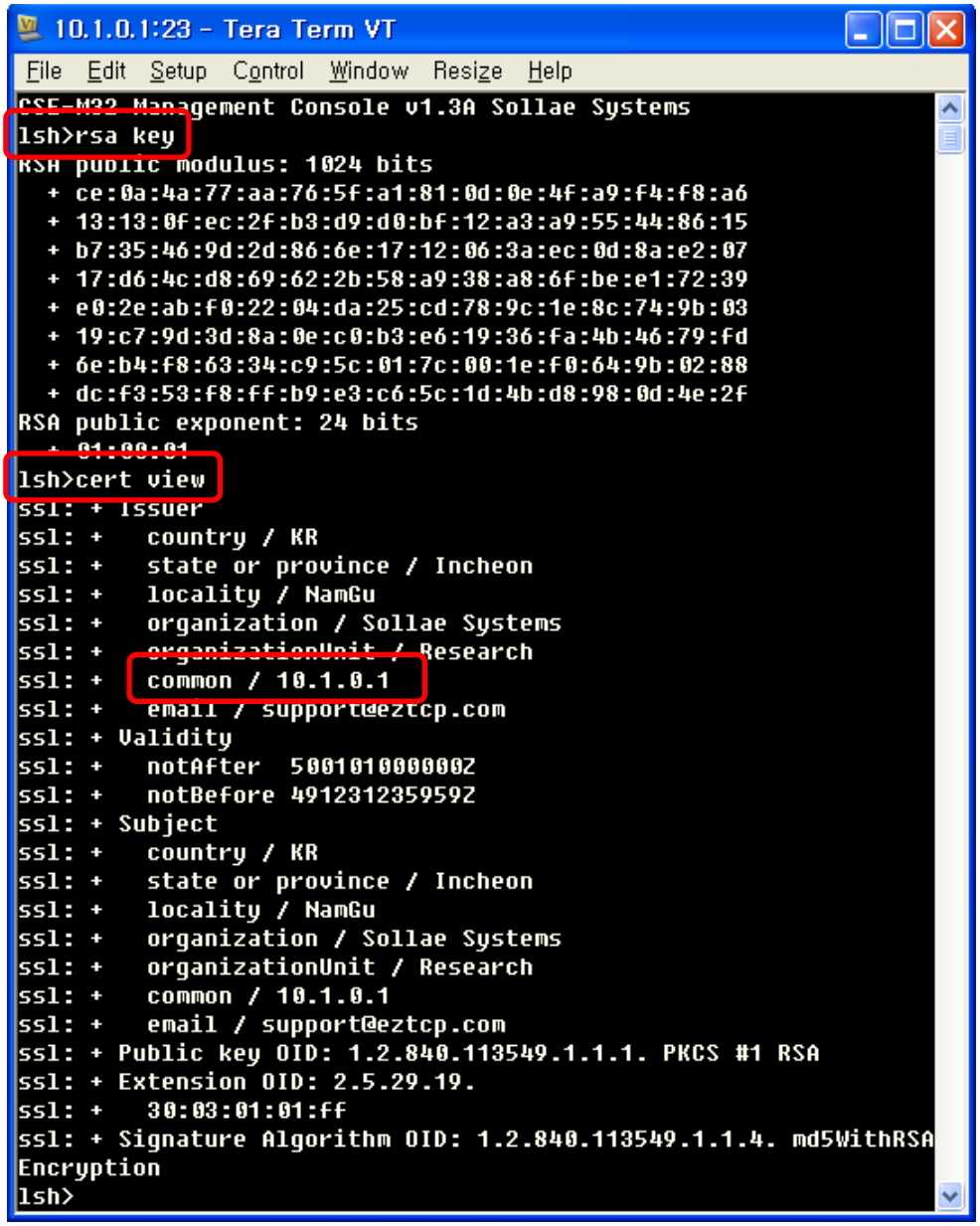

Figure 3-3 confirm RSA KEY and Certificate

3.1.3 Connecting to ezTCP

To communicate with the ezTCP enabled the SSL feature, remote host must support SSL. Confirm SSL feature by using ezVSP support SSL. The ezVSP is the Virtual Com Port Redirector, which is supplied freely.

- Setting ezVSP
  Click the [Creat an ezVSP Port] button of ezManger.

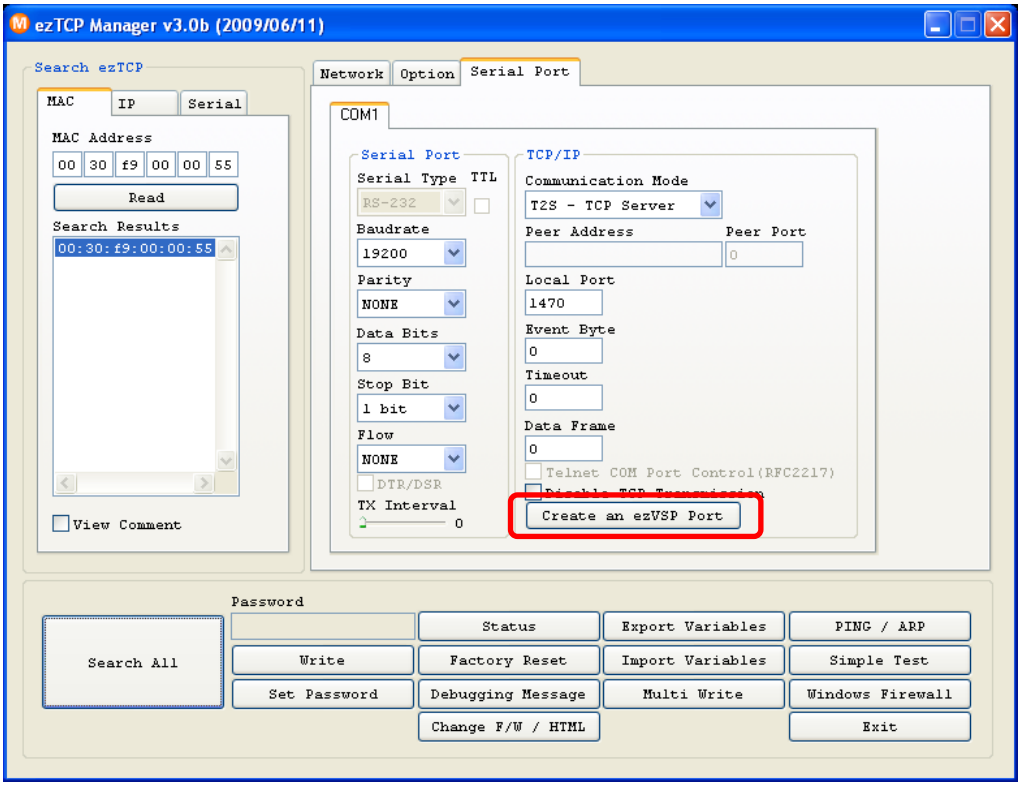

Figure 3-4 Create an VSP

Configure like the below and click [OK] button.

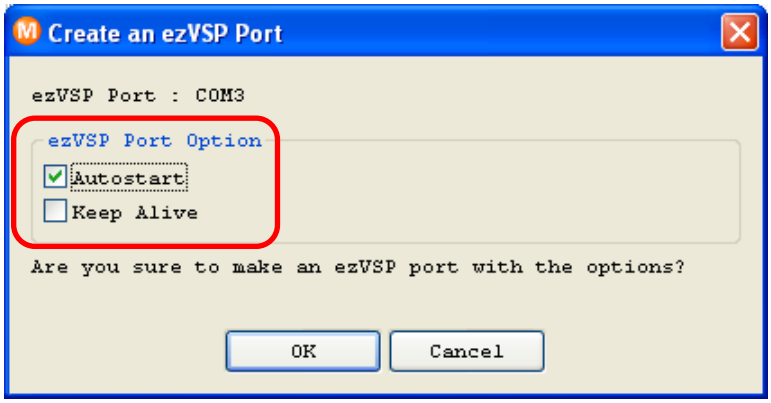

Figure 3-5 Configure an VSP

Refer to ezVSP user's manual for installing ezVSP program and details.

- Confirm TCP connection

  After start ezVSP, click the [Status] button of ezManager. User can confirm "TCP STATE" / "COM1 – ESTABLISHED" and "SSL STATUS" / "State – 7", "Cipher – RSA_AES_256_CBC_SHA".

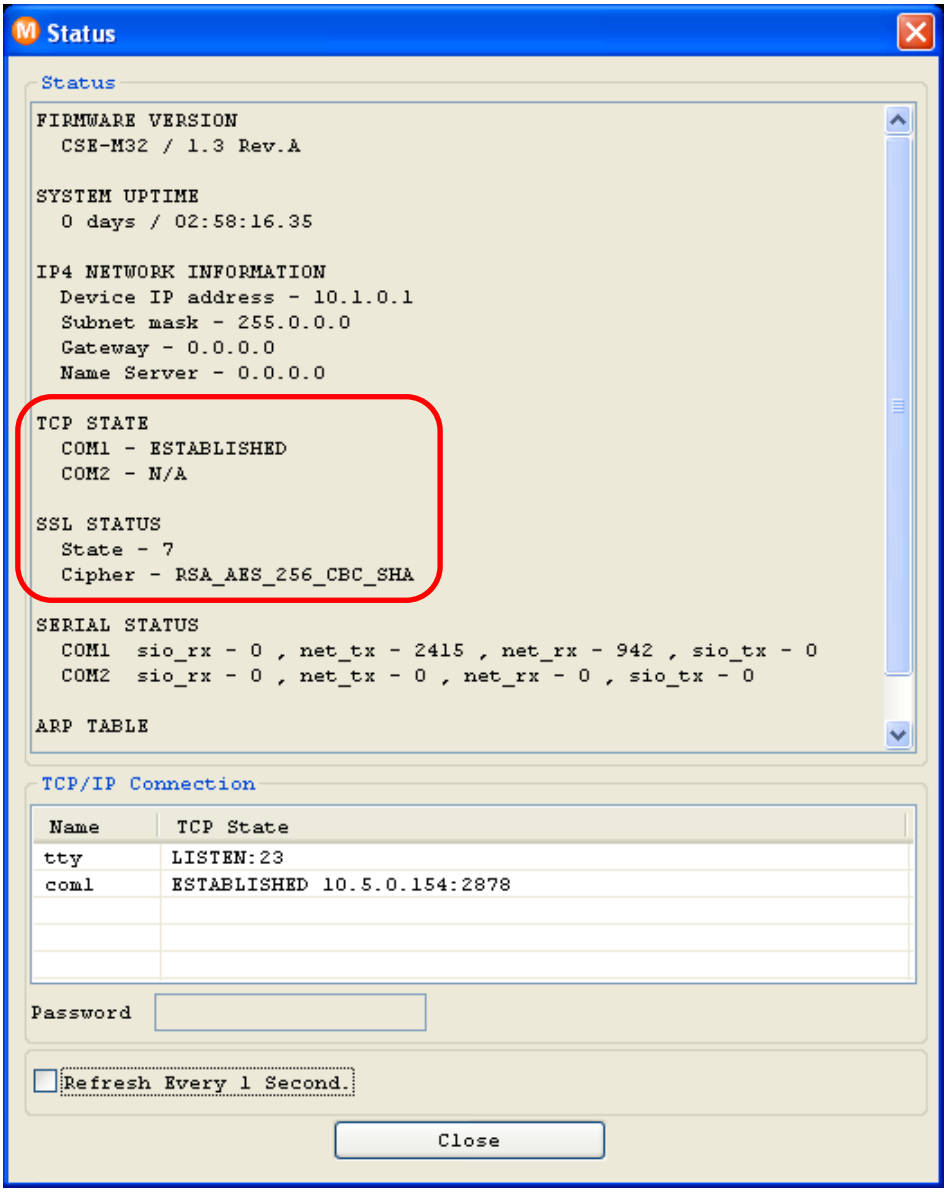

Figure 3-6 confirm TCP connection of SSL feature

3.2 TCP Client

SSL client doesn't need to make the RSA server key and the digital certificate. Therefore user can operate the ezTCP as TCP client with SSL feature by only enabling [SSL] option.

To confirm current TCP connection use the [Status] button of ezManager the same as TCP server mode.

4 Revision History

Date	Version	Comments
Sep. 16. 2008	1.0	Initial Release
Jun. 11. 2009	1.1	Modify images and terms Add product CSE-H25