EZL-400S Application Notes (002)

SSL (Secure Socket Layer)

Version 1.0

sollae Sollae Systems Co., Ltd.
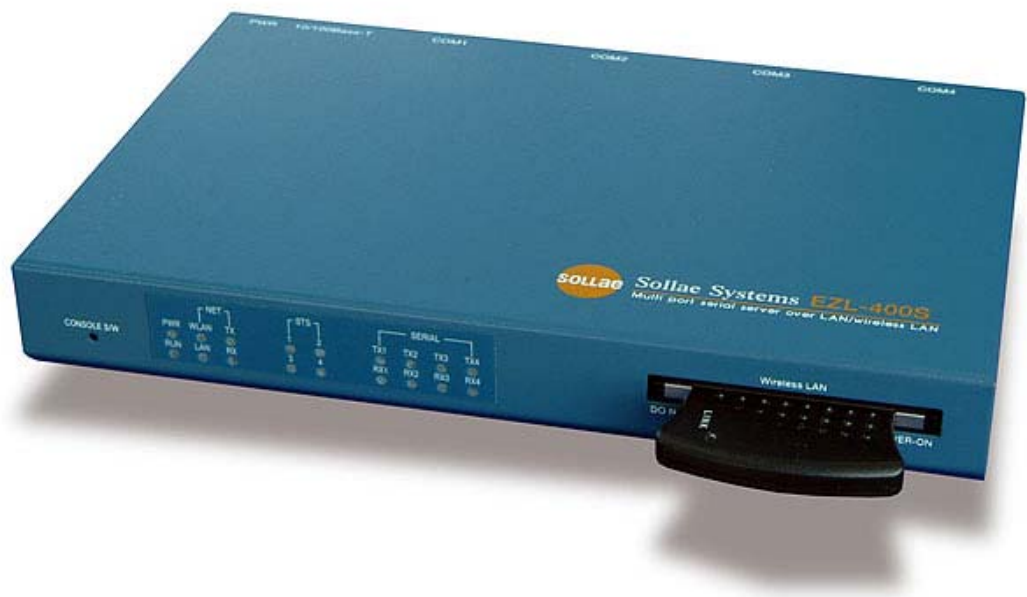
1. Using SSL in Client Mode

To use the SSL in client mode, you must log in telnet and activate SSL.
Client mode means connecting to the server in COD or ATC mode using atd command.
For client using SSL, the target server must use SSL as well.

1.1. Activating SSL

You can activate SSL after login as telnet client. The example below shows how to activate SSL.

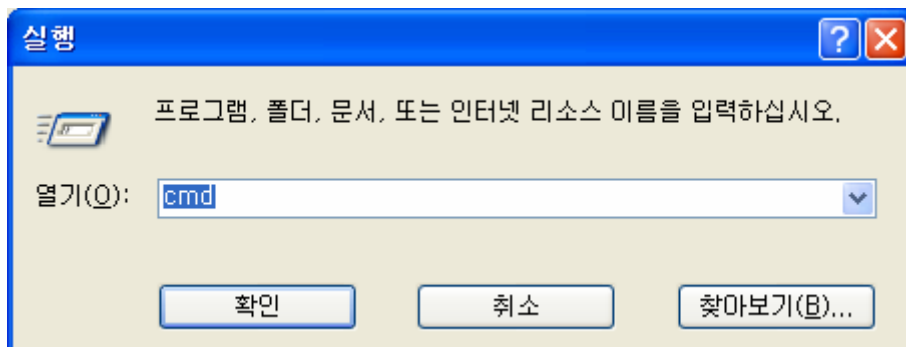### 1.1.1. Setting IP Address

You must set IP addresses for your EZL-400S environment: [LOCAL IP ADDRESS], [SUBNET MASK], and [GATEWAY IP ADDRESS].
The description in this manual assumes IP addresses for PC and EZL-400S as follows:

	PC	EZL-400S
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0
Gateway IP Address	10.1.0.254	10.1.0.254

1.1.2. telnet login

Select [Run] in the Windows [Start] menu and type 'cmd' or 'command' to start DOS session.

In the DOS window, enter:

'telnet [LOCAL IP ADDRESS]',

where [LOCAL IP ADDRESS] is the IP address of EZL-400S set in the step 1.1.1.

e.g.) telnet 10.1.0.1

The following window will be displayed after login.

1.1.3. Activating SSL

Enter 'env ext' and 'y' for 'SSL" to activate SSL.

1.1.4. Rebooting

After you set all items, the system will reboot automatically.

Even one item is updated in the console, the system will reboot automatically.

1.2.　Precautions for Client SSL Communication

1.2.1. SSL Client Communication Modes

Since SSL operates over TCP protocol, communication is allowed only in the communication modes where TCP is applied.
The communication modes which support SSL client communication include:

- COD mode
- ATC mode where 'atd' command is used

2. Using SSL in Server Mode

2.1.   Activating SSL

You can activate SSL after login as telnet client. The example below shows how to activate SSL.
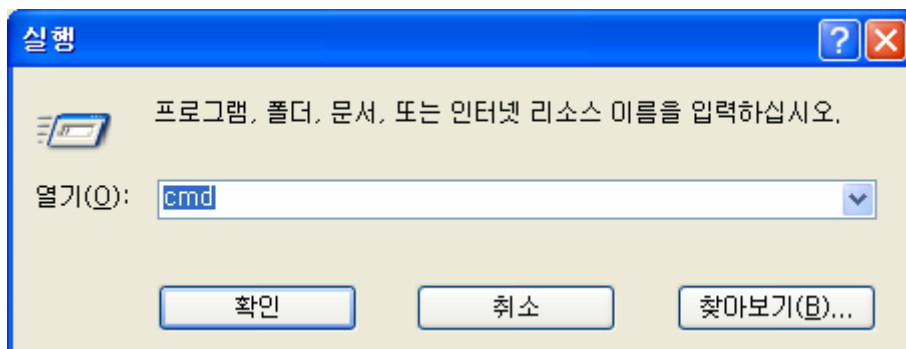
2.1.1. Setting IP Address

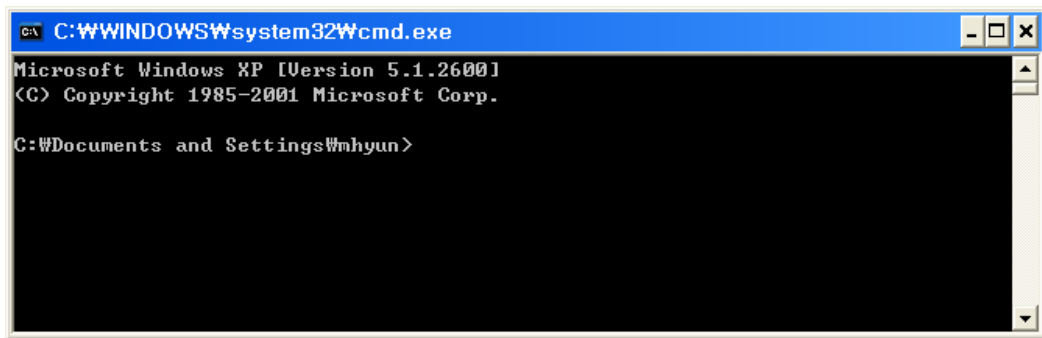You must set IP addresses for your EZL-400S environment: [LOCAL IP ADDRESS], [SUBNET MASK], and [GATEWAY IP ADDRESS].
The description in this manual assumes IP addresses for PC and EZL-400S as follows:

	PC	EZL-400S
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0
Gateway IP Address	10.1.0.254	10.1.0.254

2.1.2. telnet login

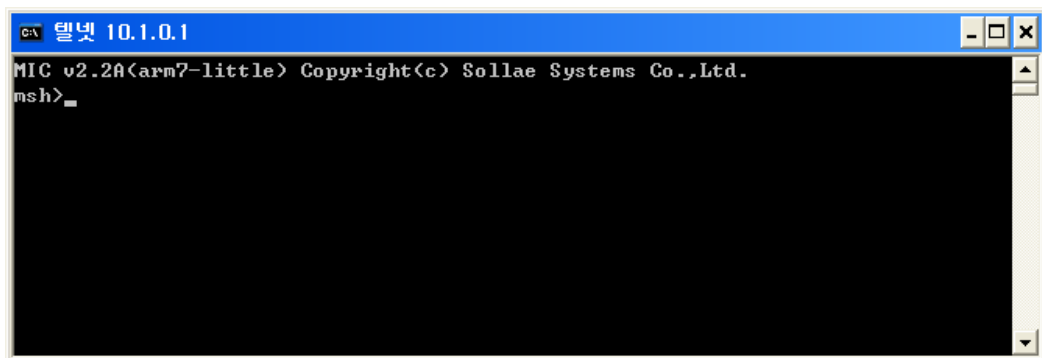Select [Run] in the Windows [Start] menu and type 'cmd' or 'command' to start DOS session.

In the DOS window, enter:

'telnet [LOCAL IP ADDRESS]',

where [LOCAL IP ADDRESS] is the IP address of EZL-400S set in the step 1.1.1.
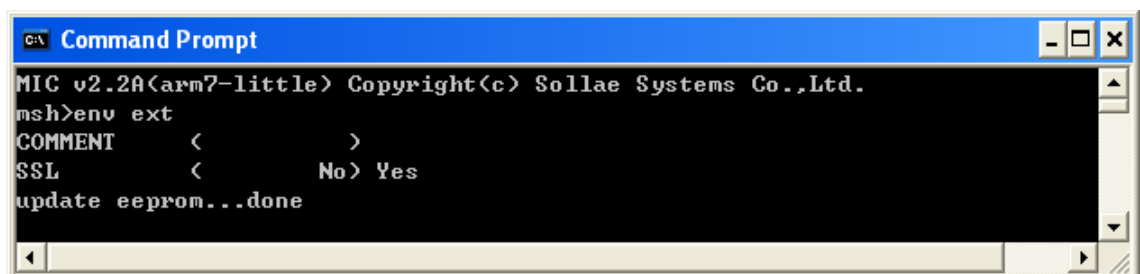
e.g.) telnet 10.1.0.1

The following window will be displayed after login.

2.1.3. Activating SSL

Enter 'env ext' and 'y' for 'SSL" to activate SSL.

2.1.4. Rebooting

After you set all items, the system will reboot automatically.

Even one item is updated in the console, the system will reboot automatically.

2.2.　　Creating Keys

To use SSL in server mode, you should create a public key for the SSL client and a private key for the SSL server.

2.2.1. telnet Login

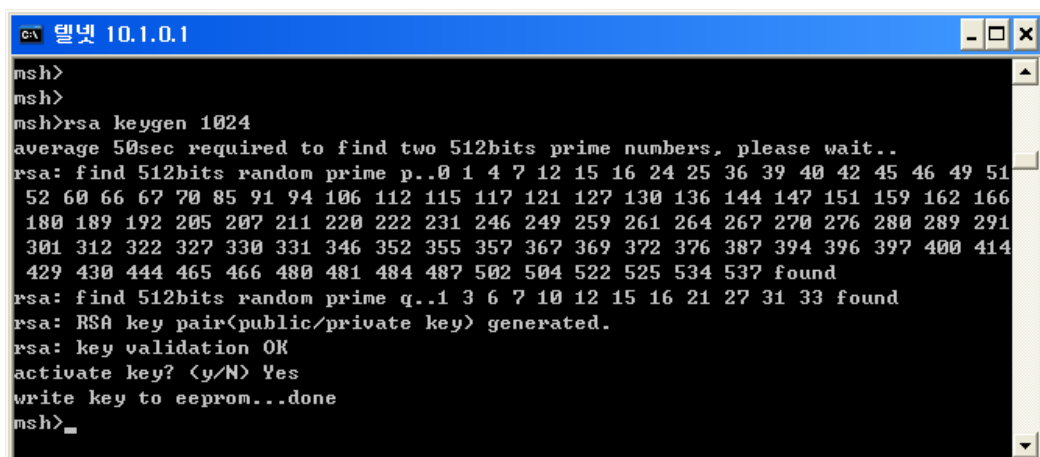If you are not logged in telnet, log in telnet as described in step 2.1.

2.2.2. Creating Keys

Create RSA key by using the following command.
(Command format) rsa keygen [keylength]
You can set [keylength] to 512, 768, 1024 or 2048.
Creating a key may take up to a few minutes depending on the key length, for example, 2048 bit length key will take about 5 minutes.
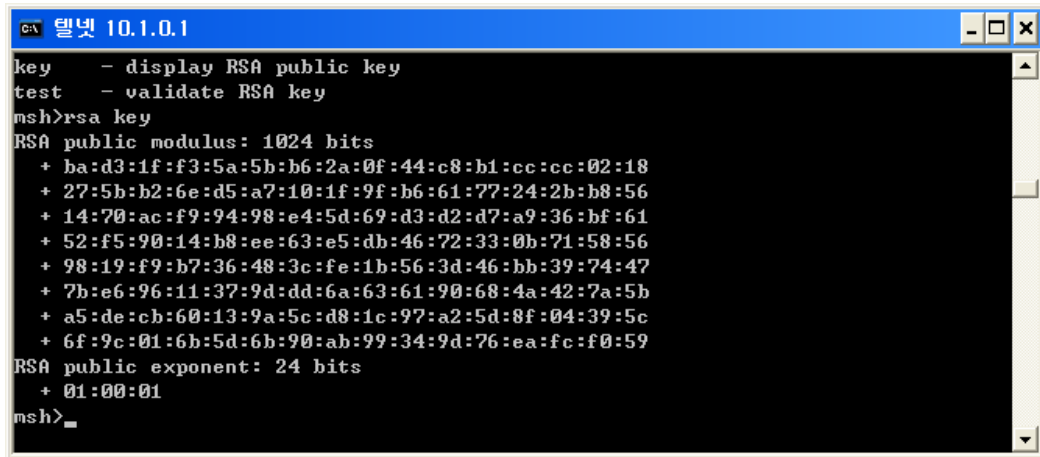
```
텔넷 10.1.0.1
msh>
msh>
msh>rsa keygen 1024
average 50sec required to find two 512bits prime numbers, please wait..
rsa: find 512bits random prime p..0 1 4 7 12 15 16 24 25 36 39 40 42 45 46 49 51
 52 60 66 67 70 85 91 94 106 112 115 117 121 127 130 136 144 147 151 159 162 166
 180 189 192 205 207 211 220 222 231 246 249 259 261 264 267 270 276 280 289 291
 301 312 322 327 330 331 346 352 355 357 367 369 372 376 387 394 396 397 400 414
 429 430 444 465 466 480 481 484 487 502 504 522 525 534 537 found
rsa: find 512bits random prime q..1 3 6 7 10 12 15 16 21 27 31 33 found
rsa: RSA key pair(public/private key) generated.
rsa: key validation OK
activate key? (y/N) Yes
write key to eeprom...done
msh>
```

After creating the key, you will be prompted to save the key in the flash memory. Press 'y' to save the key in the non-volatile memory.

2.2.3. Displaying RSA Public Key

You can display the RSA public key using 'rsa key' command.

```
텔넷 10.1.0.1                                                    _□×
key     - display RSA public key                                ▲
test    - validate RSA key
msh>rsa key
RSA public modulus: 1024 bits
  + ba:d3:1f:f3:5a:5b:b6:2a:0f:44:c8:b1:cc:cc:02:18
  + 27:5b:b2:6e:d5:a7:10:1f:9f:b6:61:77:24:2b:b8:56
  + 14:70:ac:f9:94:98:e4:5d:69:d3:d2:d7:a9:36:bf:61
  + 52:f5:90:14:b8:ee:63:e5:db:46:72:33:0b:71:58:56
  + 98:19:f9:b7:36:48:3c:fe:1b:56:3d:46:bb:39:74:47
  + 7b:e6:96:11:37:9d:dd:6a:63:61:90:68:4a:42:7a:5b
  + a5:de:cb:60:13:9a:5c:d8:1c:97:a2:5d:8f:04:39:5c
  + 6f:9c:01:6b:5d:6b:90:ab:99:34:9d:76:ea:fc:f0:59
RSA public exponent: 24 bits
  + 01:00:01
msh>_                                                           ▼
```

2.2.4. Testing RSA Key

You can test private and public RSA keys you have created. Use the public key to encrypt a text. Use the private key to decrypt the encrypted text and check that both texts are identical.

Now use the private key to encrypt a text. Use the public key to decrypt the encrypted text and check that both texts are identical.

2.3.   Creating Certificate

The SSL server should have a certificate. You can create and use an authorized certificate.

2.3.1. Creating Certificate

You can create a certificate using 'cert new' command. EZL-400S will create and sign a certificate for 'cert new' command. When certificate is created, you will be prompted to save the created certificate in the nonvolatile memory. Press 'y' to store the certificate in the nonvolatile memory.

Since certificates contain IP address information, you have to create a new certificate whenever you change the IP address.