EZL-200F Application Notes (002)

SSL (Secure Socket Layer)

Version 2.0

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.

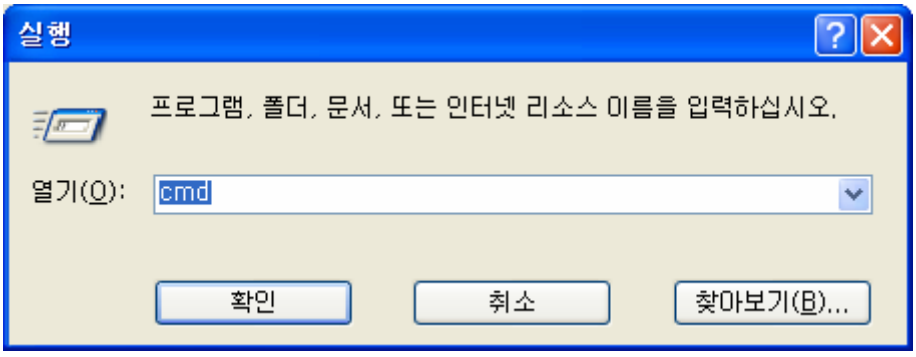
1.1.1. Setting IP Address

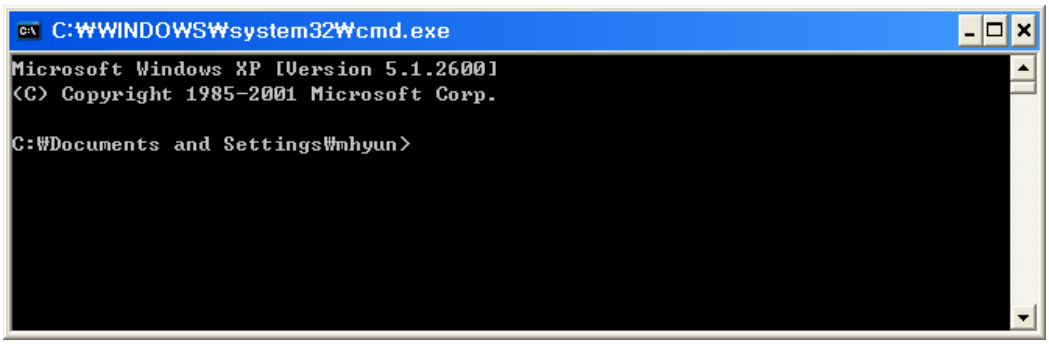
You must set IP addresses for your EZL-200F environment: [LOCAL IP ADDRESS], [SUBNET MASK], and [GATEWAY IP ADDRESS].
The description in this manual assumes IP addresses for PC and EZL-200F as follows:

	PC	EZL-200F
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.





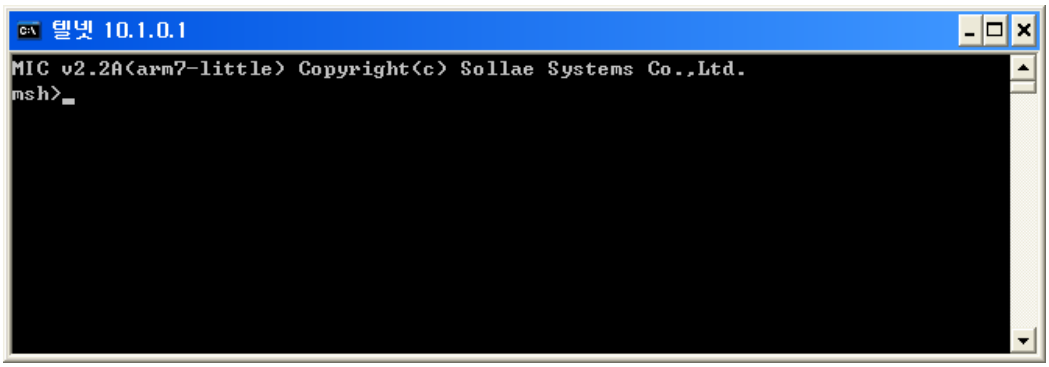
In the DOS window, enter:

'telnet [LOCAL IP ADDRESS]',

where [LOCAL IP ADDRESS] is the IP address of EZL-200F 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.

Press [ENTER] for other items.

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.

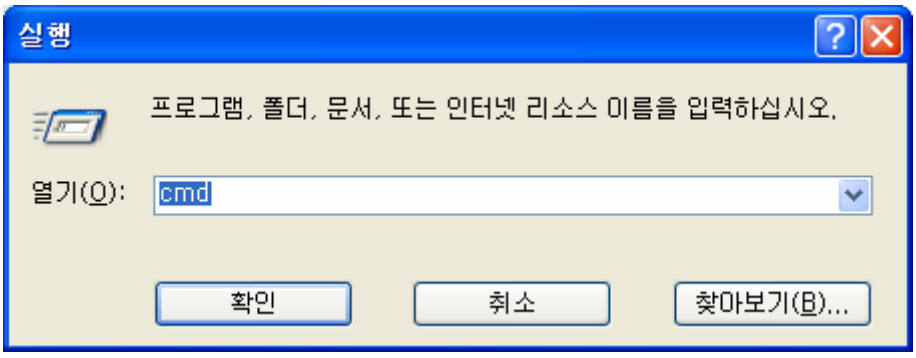
2.1.1. Setting IP Address

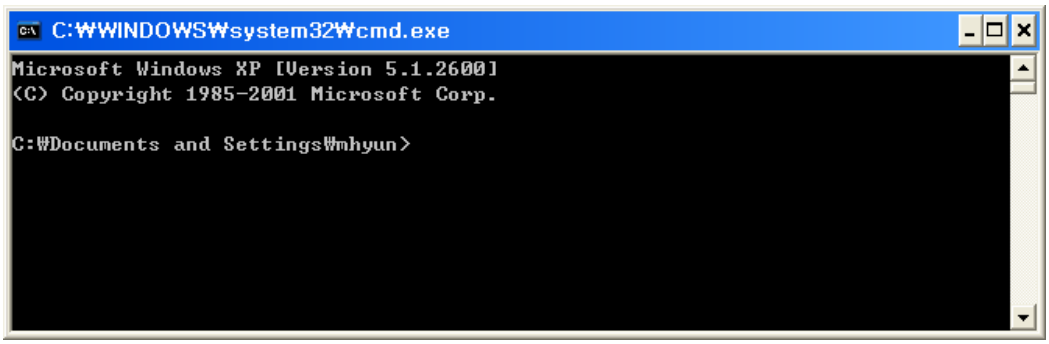
You must set IP addresses for your EZL-200F environment: [LOCAL IP ADDRESS], [SUBNET MASK], and [GATEWAY IP ADDRESS].
The description in this manual assumes IP addresses for PC and EZL-200F as follows:

	PC	EZL-200F
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.





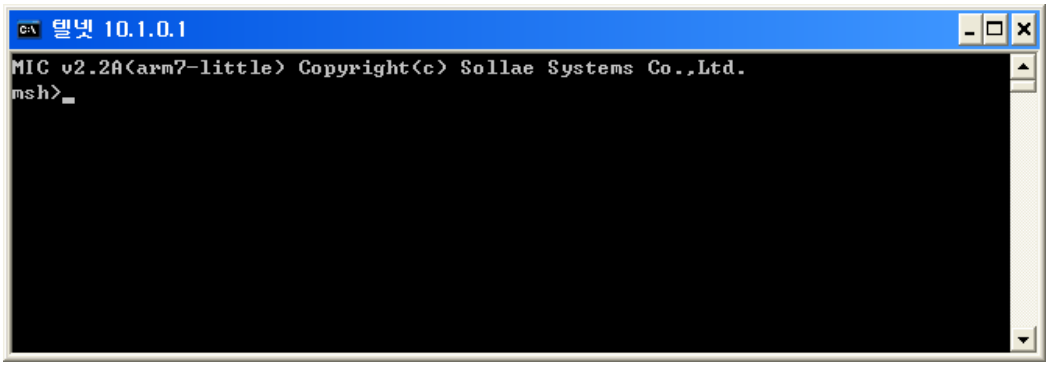
In the DOS window, enter:

'telnet [LOCAL IP ADDRESS]',

where [LOCAL IP ADDRESS] is the IP address of EZL-200F 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.

Press [ENTER] for other items.

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

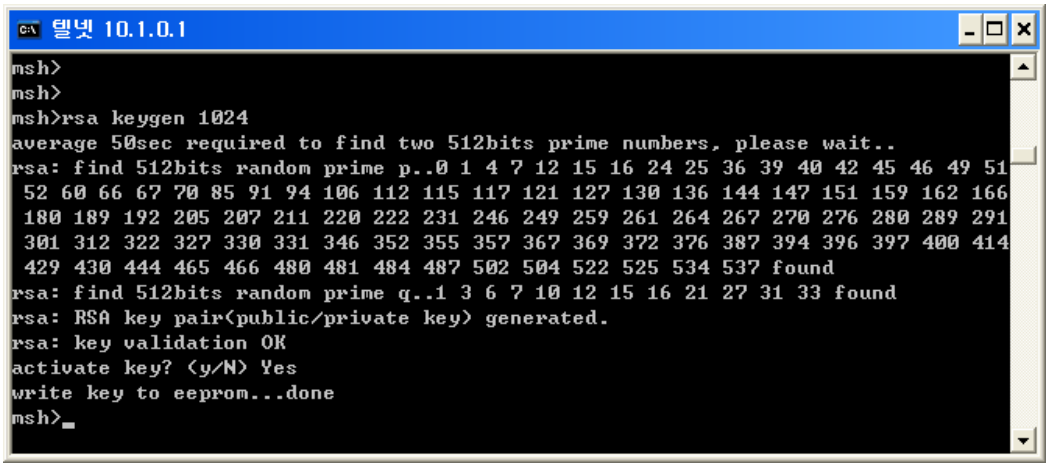
To use SSL in server mode, you should create a public key for the SSL client and a private key for the SSL server.

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

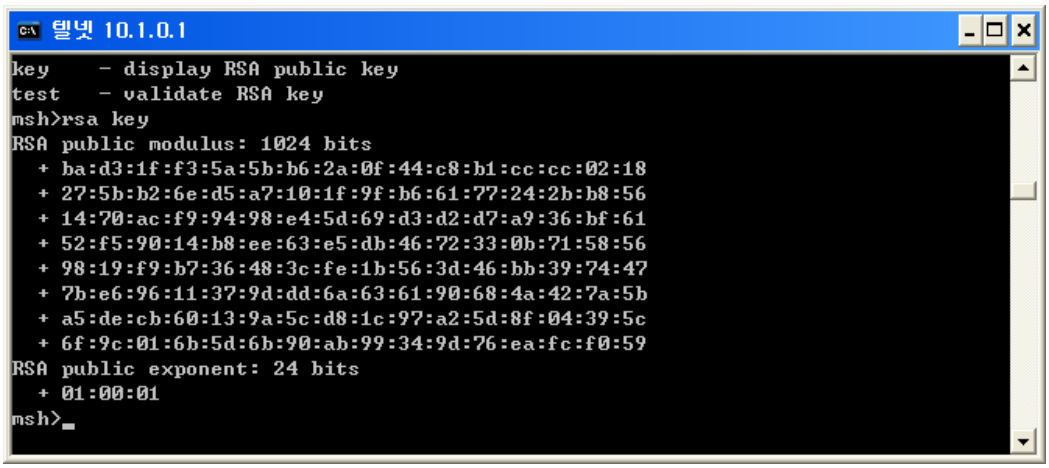
Create RSA key by using the following command.
(Command format) rsa keygen [keylength]
You can set [keylength] to 512, 768, 1024 or 2048.
Creating a key may take up to a few minutes depending on the key length, for example, 2048 bit length key will take about 5 minutes.



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

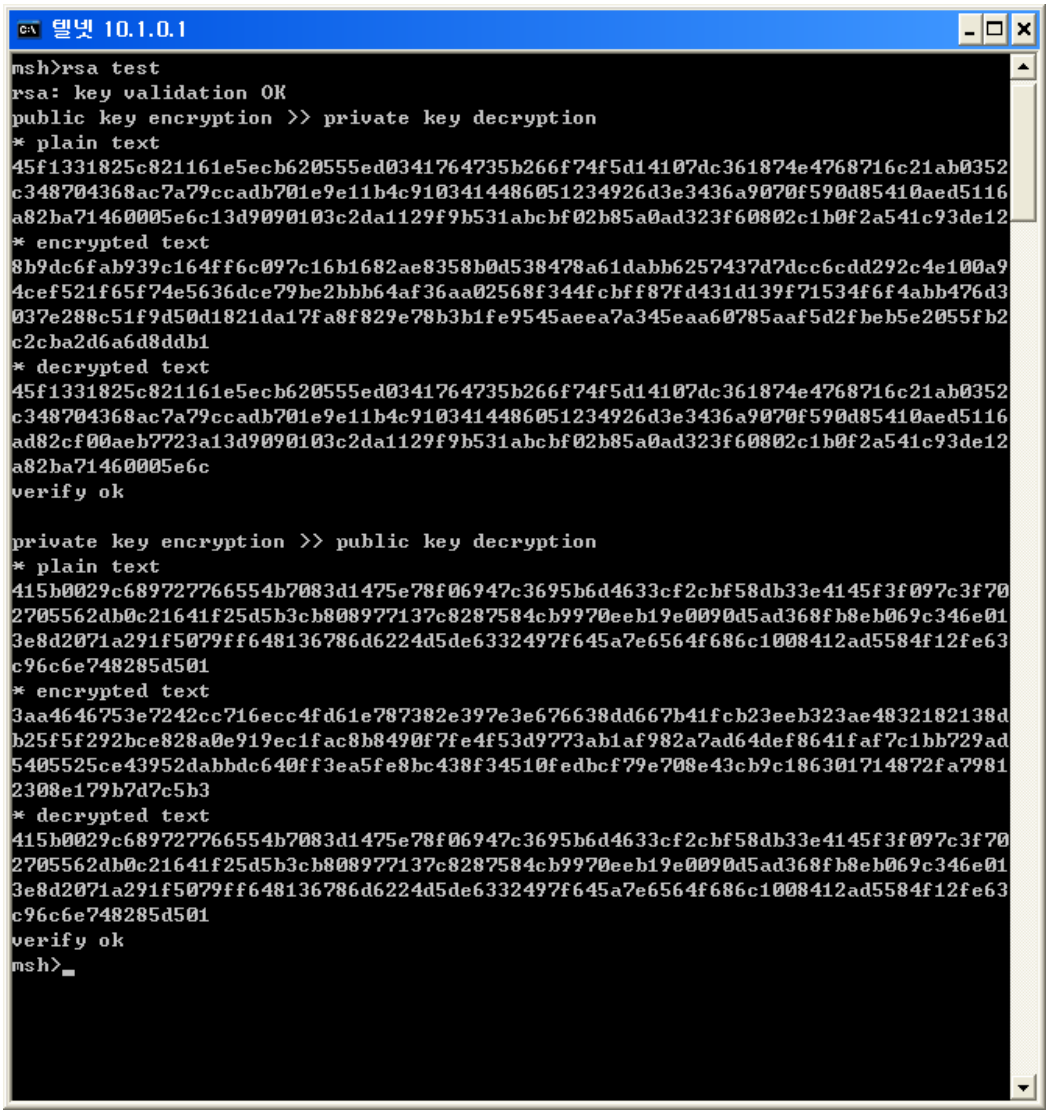
You can display the RSA public key using ‘rsa key’ command.



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.

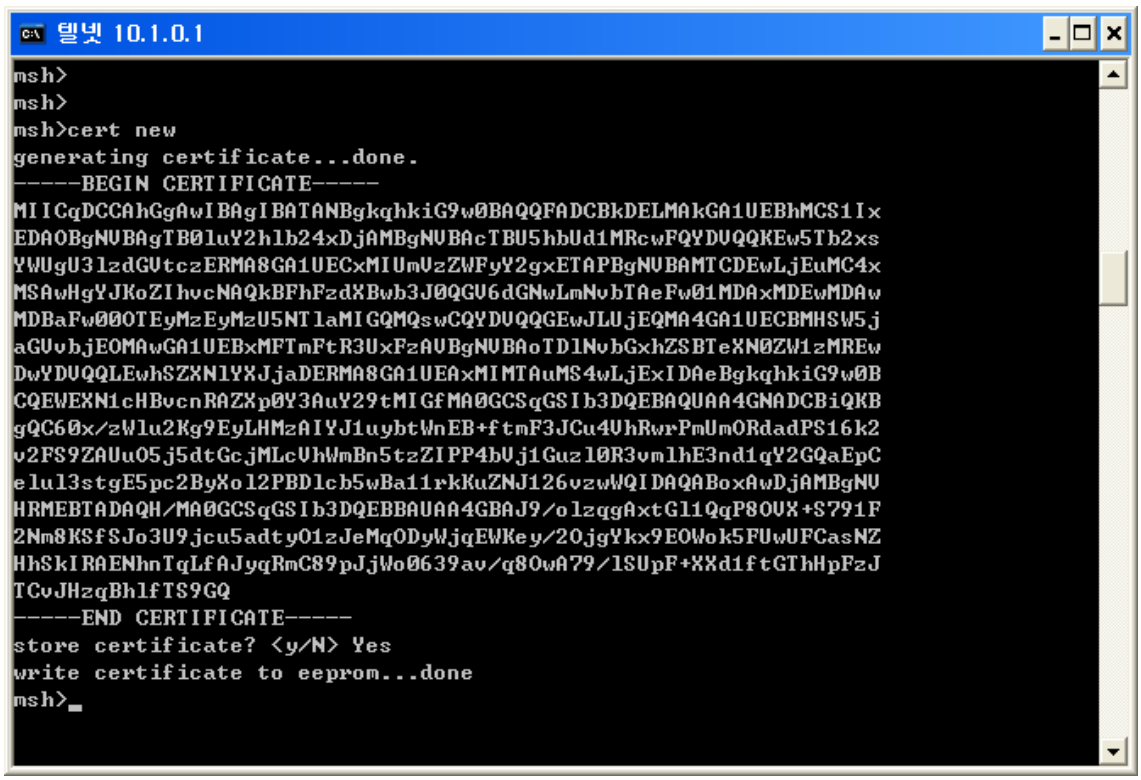


2.3. Creating Certificate

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-200F 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.

3. Revision History

Date	Version	Comments
Jun.13.2005	1.0	The first release
Dec.06.2005	2.0	Added revision history Changed all fonts into Times New Roman