

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

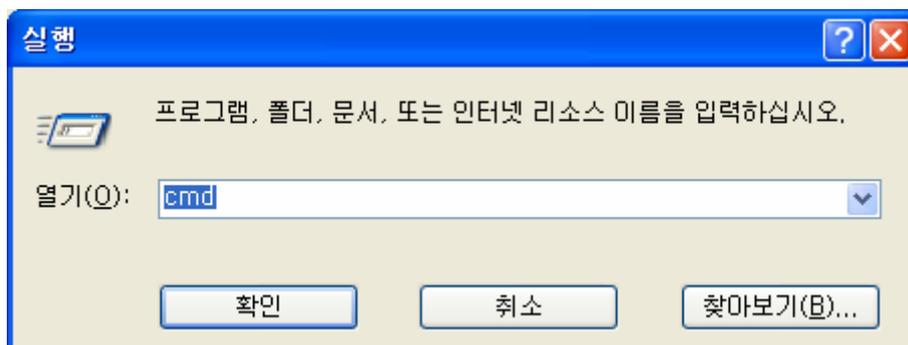
You must set IP addresses for your EZL-200F environment: [LOCAL IP ADDRESS], [SUBNET MASK], and [GATEWAY IP ADDRESS].

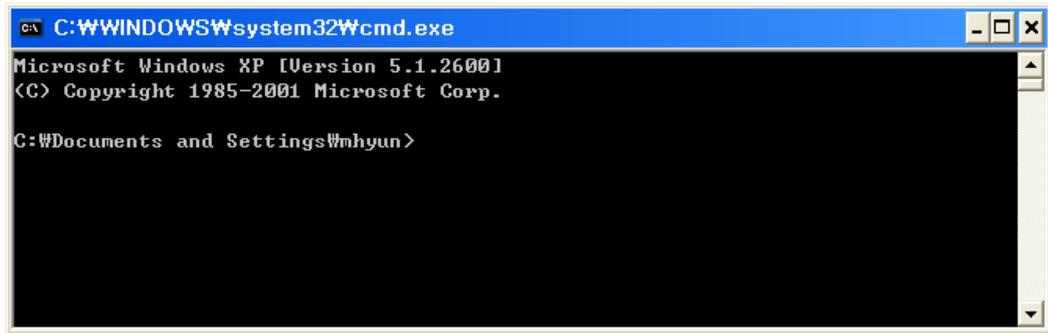
The description in this manual assumes IP addresses for PC and EZL-200F as follows:

	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.





```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Wmhyun>
```

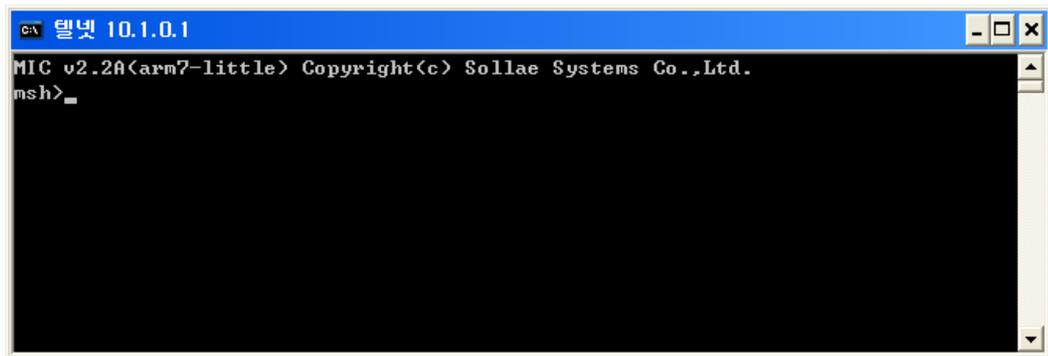
In the DOS window, enter:

'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.



```
텔넷 10.1.0.1
MIC v2.2A(arm7-little) Copyright(c) Sollae Systems Co.,Ltd.
msh>
```

1.1.3. Activating SSL

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



```
텔넷 10.1.0.1
MIC v2.2A(arm7-little) Copyright(c) Sollae Systems Co.,Ltd.
msh>env ext
COMMENT      <          >
SSL          <      No > Yes
SEND DELAY  <      0 > _
```

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

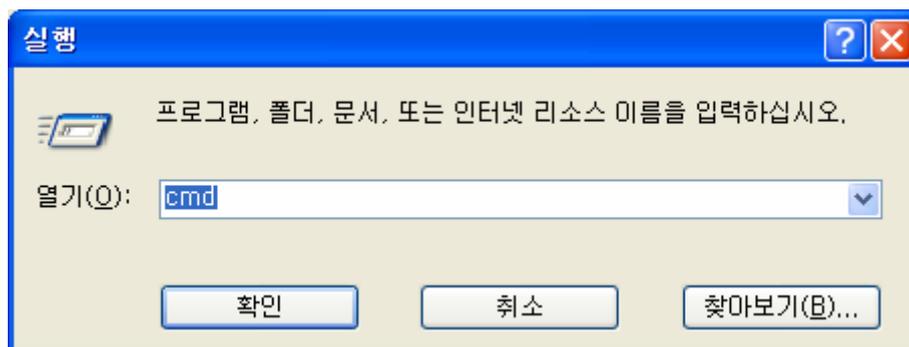
You must set IP addresses for your EZL-200F environment: [LOCAL IP ADDRESS], [SUBNET MASK], and [GATEWAY IP ADDRESS].

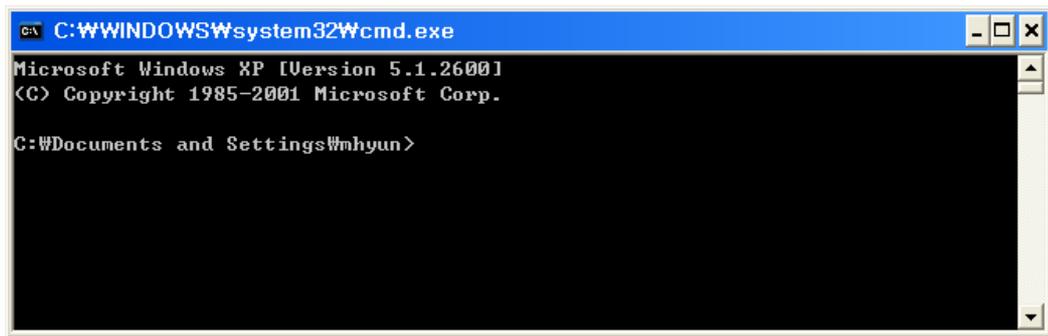
The description in this manual assumes IP addresses for PC and EZL-200F as follows:

	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.





```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.26001]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Wmhyun>
```

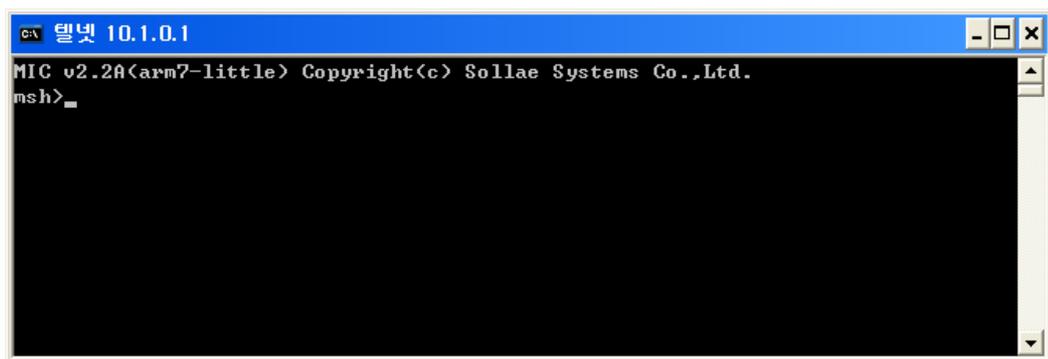
In the DOS window, enter:

'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.



```
텔넷 10.1.0.1
MIC v2.2A(arm7-little) Copyright(c) Sollae Systems Co.,Ltd.
msh>
```

2.1.3. Activating SSL

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



```
텔넷 10.1.0.1
MIC v2.2A(arm7-little) Copyright(c) Sollae Systems Co.,Ltd.
msh>env ext
COMMENT      <          >
SSL          <      No > Yes
SEND DELAY   <      0 > _
```

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.

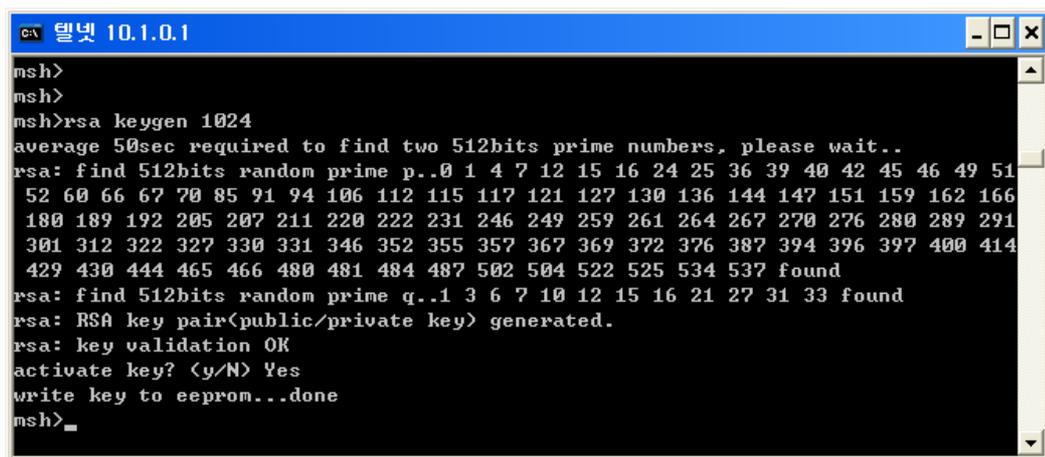
2.2.2. Creating Keys

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.

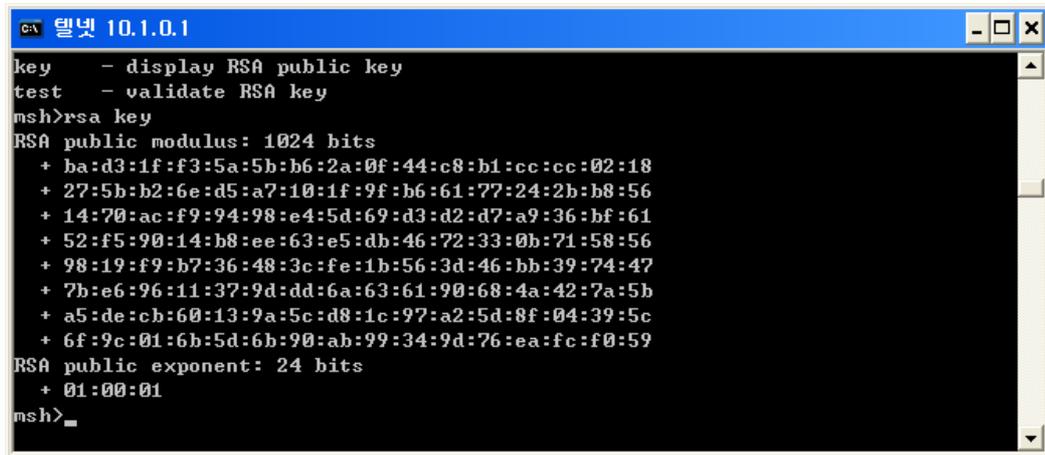


```
ca 텔넷 10.1.0.1
msh>
msh>
msh>rsa keygen 1024
average 50sec required to find two 512bits prime numbers, please wait..
rsa: find 512bits random prime p..0 1 4 7 12 15 16 24 25 36 39 40 42 45 46 49 51
52 60 66 67 70 85 91 94 106 112 115 117 121 127 130 136 144 147 151 159 162 166
180 189 192 205 207 211 220 222 231 246 249 259 261 264 267 270 276 280 289 291
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.



```
CA 달넷 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.

```
CA 텔넷 10.1.0.1
msh>rsa test
rsa: key validation OK
public key encryption >> private key decryption
* plain text
45f1331825c821161e5ecb620555ed0341764735b266f74f5d14107dc361874e4768716c21ab0352
c348704368ac7a79ccadb701e9e11b4c9103414486051234926d3e3436a9070f590d85410aed5116
a82ba71460005e6c13d9090103c2da1129f9b531abcbf02b85a0ad323f60802c1b0f2a541c93de12
* encrypted text
8b9dc6fab939c164ff6c097c16b1682ae8358b0d538478a61dabb6257437d7dcc6cdd292c4e100a9
4cef521f65f74e5636dce79be2bbb64af36aa02568f344fcbff87fd431d139f71534f6f4abb476d3
037e288c51f9d50d1821da17fa8f829e78b3b1fe9545aea7a345aa60785aaf5d2fbeb5e2055fb2
c2cba2d6a6d8ddb1
* decrypted text
45f1331825c821161e5ecb620555ed0341764735b266f74f5d14107dc361874e4768716c21ab0352
c348704368ac7a79ccadb701e9e11b4c9103414486051234926d3e3436a9070f590d85410aed5116
ad82cf00aeb7723a13d9090103c2da1129f9b531abcbf02b85a0ad323f60802c1b0f2a541c93de12
a82ba71460005e6c
verify ok

private key encryption >> public key decryption
* plain text
415b0029c689727766554b7083d1475e78f06947c3695b6d4633cf2cbf58db33e4145f3f097c3f70
2705562db0c21641f25d5b3cb808977137c8287584cb9970eeb19e0090d5ad368fb8eb069c346e01
3e8d2071a291f5079ff648136786d6224d5de6332497f645a7e6564f686c1008412ad5584f12fe63
c96c6e748285d501
* encrypted text
3aa4646753e7242cc716ecc4fd61e787382e397e3e676638dd667b41fcb23eeb323ae4832182138d
b25f5f292bce828a0e919ec1fac8b8490f7fe4f53d9773ab1af982a7ad64def8641faf7c1bb729ad
5405525ce43952dabbd640ff3ea5fe8bc438f34510fedbcf79e708e43cb9c186301714872fa7981
2308e179b7d7c5b3
* decrypted text
415b0029c689727766554b7083d1475e78f06947c3695b6d4633cf2cbf58db33e4145f3f097c3f70
2705562db0c21641f25d5b3cb808977137c8287584cb9970eeb19e0090d5ad368fb8eb069c346e01
3e8d2071a291f5079ff648136786d6224d5de6332497f645a7e6564f686c1008412ad5584f12fe63
c96c6e748285d501
verify ok
msh>
```

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.

```

c:\> 텔넷 10.1.0.1
msh>
msh>
msh>cert new
generating certificate...done.
-----BEGIN CERTIFICATE-----
MIICqDCCAhGgAwIBAgIBATANBgkqhkiG9w0BAQQFAQCBkDELMAkGA1UEBhMCS1Ix
EDA0BgNUBAGTB01uY2h1b24xDjAMBgNVBAcTBu5hbUd1MRcwFQYDUQQKEw5Tb2xs
YWUgU3lzdGUtczERMA8GA1UECzMlUmVzZWZyY2gyETAPBgNVBAMTCDEwLjEwLjEw
MSAwHgYJKoZIhvcNAQkBFhFzdXBwY290LjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
MDEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
aGUvbyJEMAAwGA1UEBxMFTmFtR3UxPzAUBgNVBAoTD1NvbGxhZSBTeXN0ZW1zMREw
DwYDUQQLEWhSZXN1YXJjaDERMA8GA1UEAxMI MTAuMS4wLjEwLjEwLjEwLjEwLjEwLjEw
CQEWEXN1cHBvcnRAZXp0Y3AuY290tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC60x/zWlu2Kg9EyLHMzAIYJ1uybtWnEB+ftmF3JCu4UhrRwPmUmORdadPS16k2
v2FS9ZAUu05j5dtGcJMLcVhWmBn5tzZIPP4bVj1Guz10R3vm1hE3nd1qY2GQaEpC
e1u13stgE5pc2ByXo12PBD1cb5wBa11rkKuZMJ126vzwWQIDAQABoxAwDjAMBgNV
HRMEBTAQAQH/MA0GCSqGSIb3DQEBAQUAA4GBAJ9/o1zqqAxtG11QqP8OUX+S791F
2Nm8KSfsJo3U9jcu5adtY01zJemqODyWjqEWKey/20jgYkx9EOWok5FUwUFCasNZ
HhSkIRAEHhTqLFAJyqRmC89pJjWo0639av/q80wA79/1SUpF+XXd1ftGThHpFzJ
TCvJHzqBh1fTS9GQ
-----END CERTIFICATE-----
store certificate? <y/N> Yes
write certificate to eeprom...done
msh>_

```

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