

Application Note

SSH (Secure Shell) - data

Version 1.1

Sollae Systems Co., Ltd.

<http://www.ezTCP.com>

Contents

1	INTRODUCTION	- 2 -
1.1	Terminology	- 2 -
1.2	SSH (Secure Shell)	- 2 -
1.3	The ezTCP operation	- 2 -
1.4	SSH with the ezTCP	- 2 -
2	SETTING	- 3 -
2.1	Limitations	- 3 -
2.2	Set up "SSH" feature	- 3 -
2.2.1	<i>Setting with ezManager</i>	<i>- 3 -</i>
2.2.2	<i>KEY generation</i>	<i>- 4 -</i>
3	EXAMPLE OF USE	- 7 -
3.1	Confirm setting	- 7 -
3.1.1	<i>Confirm setting with ezManager</i>	<i>- 7 -</i>
3.1.2	<i>Confirm setting with telnet console</i>	<i>- 8 -</i>
3.1.3	<i>Connecting to the ezTCP</i>	<i>- 9 -</i>
3.2	Communication test	- 11 -
3.2.1	<i>Putty terminal</i>	<i>- 12 -</i>
3.2.2	<i>Serial terminal</i>	<i>- 12 -</i>
4	REVISION HISTORY	- 13 -



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 SSH (Secure Shell)

The Secure Shell (SSH) is a network protocol for providing a secure channel between two networked hosts. It is widely used for security in currently Internet environment and latest version of SSH is 2.0.

1.3 The ezTCP operation

The ezTCP has four operation mode called "ezTCP Mode" for TCP/IP communication like T2S(0), ATC(1), COD(2) and U2S(3). Each ezTCP Mode operates as below.

ezTCP Mode	TCP/IP
T2S(0)	TCP Server only
ATC(1)	TCP(both Server and Client)
COD(2)	TCP Client only
U2S(3)	UDP

1.4 SSH with the ezTCP

Originally SSH was designed as a replacement for exiting insecure remote shells, ex) TELNET. This application note introduces the SSH feature in ezTCP for data communication channel-not remote shells channel (refer to EZL-200F's application note for the SSH feature of originally purpose). The ezTCP guarantees the security of communications on Internet by supporting SSH 2.0. The products which support this feature are CSE-M32, CSE-M73, CSE-H20, CSE-H21 and CSE-H25.

2 Setting

2.1 Limitations

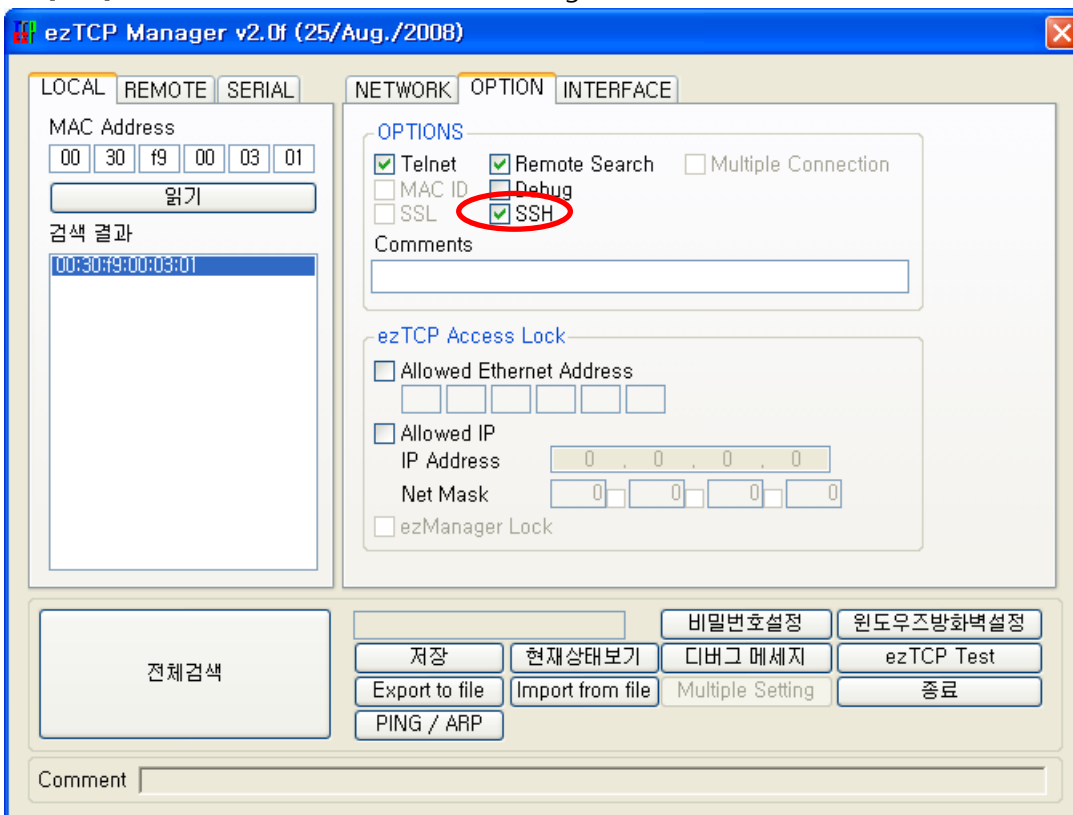
- Activate only in "T2S(0) – TCP Server" ezTCP Mode
- User cannot use below features
SSL, Telnet COM Port Control Option
- Restrictions while using "SSH" feature by each products
<CSE-M32, CSE-H20, CSE-H21>
– COM2 serial port is disabled
<CSE-M73, CSE-H25>
– "Multi Monitoring" feature is disabled

2.2 Set up "SSH" feature

SSH function is only available in TCP server mode.

2.2.1 Setting with ezManager

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

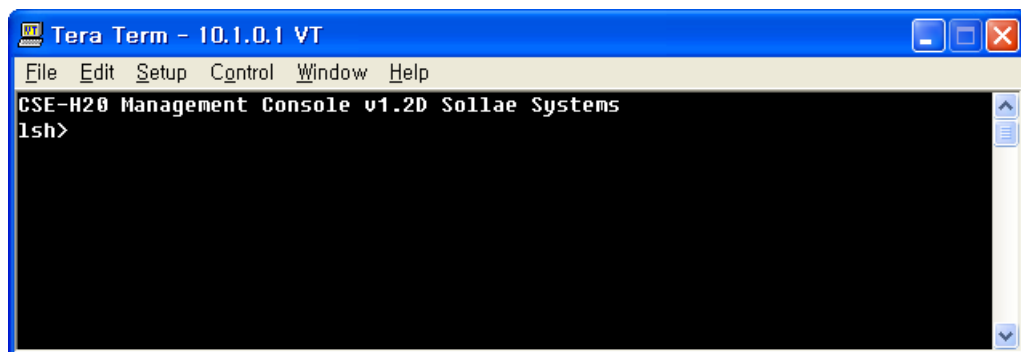


2.2.2 KEY generation

- 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
DSA KEY	dsa keygen	Generate DSA KEY
	dsa key	Confirm generated DSA KEY
ID/PW	ssh id	Set up login ID & Password
Save	ssh save aa55cc33	Save the configuration of SSH related parameter

- Log in the telnet console of the ezTCP.



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.

- RSA KEY generation
Generate RSA KEY first than DSA KEY. 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.

```

Tera Term - 10.1.0.1 VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
[sh]rsa keygen 1024
average 50sec required to find two 512bits prime numbers, please wait..
rsa: find 512bits random prime p..1 2 4 11 13 16 17 22 23 26 32 41 52 53 59
64 68 71 74 82 83 92 94 97 101 104 131 136 142 143 148 149 157 176 178 179 1
84 187 202 206 211 223 236 239 241 244 257 263 274 284 286 289 298 317 328 3
32 334 344 353 356 368 374 379 386 389 391 394 404 407 412 416 421 422 431 4
39 442 443 446 449 472 473 478 484 487 533 538 547 559 562 563 577 583 586 5
87 592 599 604 607 613 617 626 628 631 643 652 653 659 668 677 683 694 698 7
09 716 727 731 734 739 746 764 769 772 778 781 794 808 818 823 829 838 856 8
57 859 878 902 904 907 908 913 914 916 929 937 949 956 976 977 991 1003 1004
1012 1021 1024 1027 1031 1033 1034 1037 1046 1051 1058 1079 1088 1091 1094
1097 1103 1108 1111 1117 1123 1138 1142 1144 1154 1157 1163 1168 1174 1181 1
186 1192 1214 1222 1223 1229 1238 1277 1297 1301 1303 1304 1307 1313 1322 13
39 1342 1343 1346 1348 1361 1369 1376 1378 1391 1394 1403 1408 1409 found
rsa: find 512bits random prime q..1 2 7 13 14 17 22 26 29 31 34 38 44 47 59
61 64 71 73 76 77 83 86 92 97 98 106 122 133 142 149 157 163 167 176 187 188
191 196 203 211 212 226 229 233 238 241 248 254 259 274 281 286 299 301 304
313 331 332 337 343 344 346 352 353 356 359 362 373 377 383 386 388 391 394
401 406 409 412 416 421 423 442 443 446 449 458 467 479 482 497 509 511 523
524 539 541 544 551 559 566 577 584 586 587 593 598 616 632 638 644 found
rsa: RSA key pair(public/private key) generated.
rsa: key validation OK
[sh]

```

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.

- DSA KEY generation

If RSA KEY is generated successfully, generate DSA KEY by "dsa keygen" command. The KEY length filed doesn't need. The present generated DSA KEY can confirm by "dsa key" command.

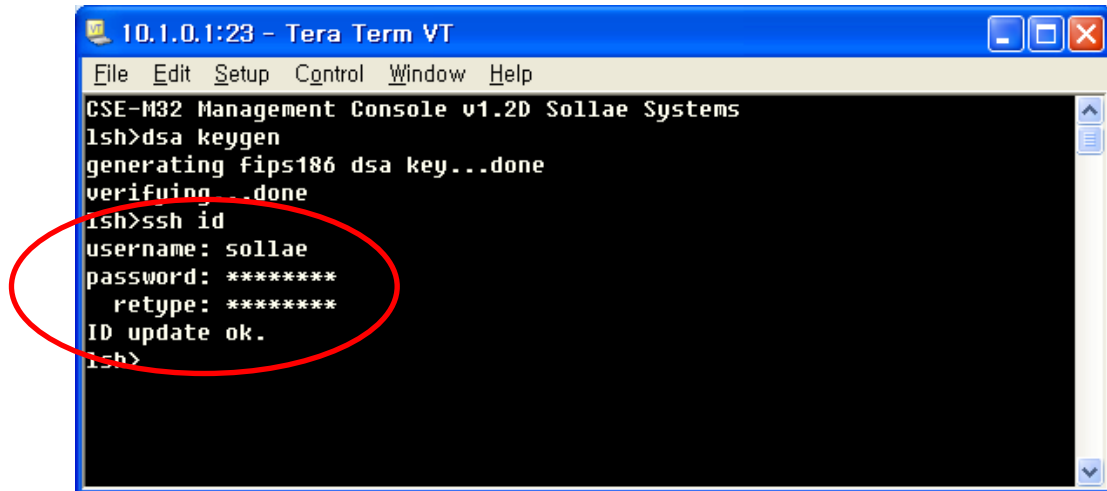
```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
[sn]dsa keygen
generating fips186 dsa key...done
verifying...done
[sn]

```

- Set up login ID and password

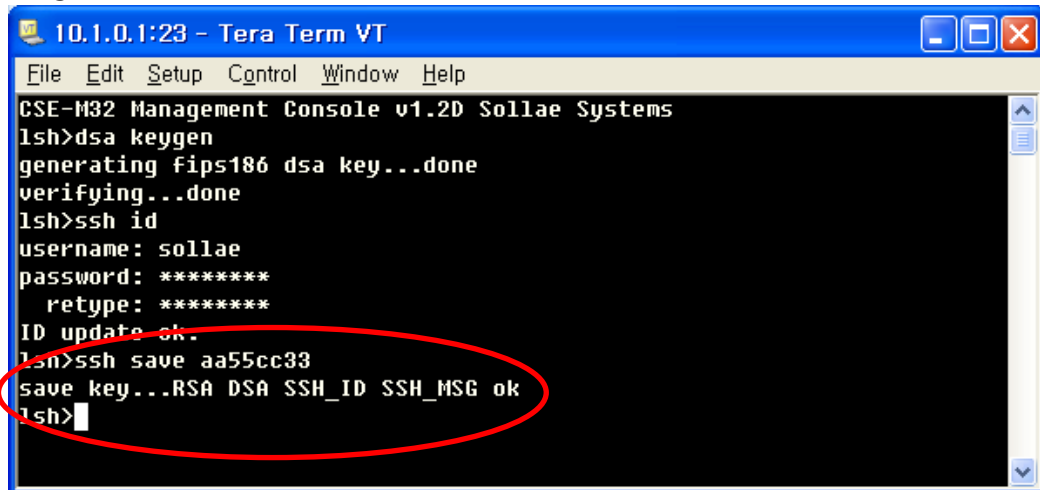
Set up ID and password by "ssh id" command for "SSH" login.



```
10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
lsh>dsa keygen
generating fips186 dsa key...done
verifying...done
lsh>ssh id
username: sollae
password: *****
retype: *****
ID update ok.
lsh>
```

- Save the configuration

The user has to save the RSA KEY, DSA KEY and ID/PW to the flash memory of ezTCP for using "SSH" feature. The command form is "ssh save aa55cc33".



```
10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
lsh>dsa keygen
generating fips186 dsa key...done
verifying...done
lsh>ssh id
username: sollae
password: *****
retype: *****
ID update ok.
lsh>ssh save aa55cc33
save key...RSA DSA SSH_ID SSH_MSG ok
lsh>
```

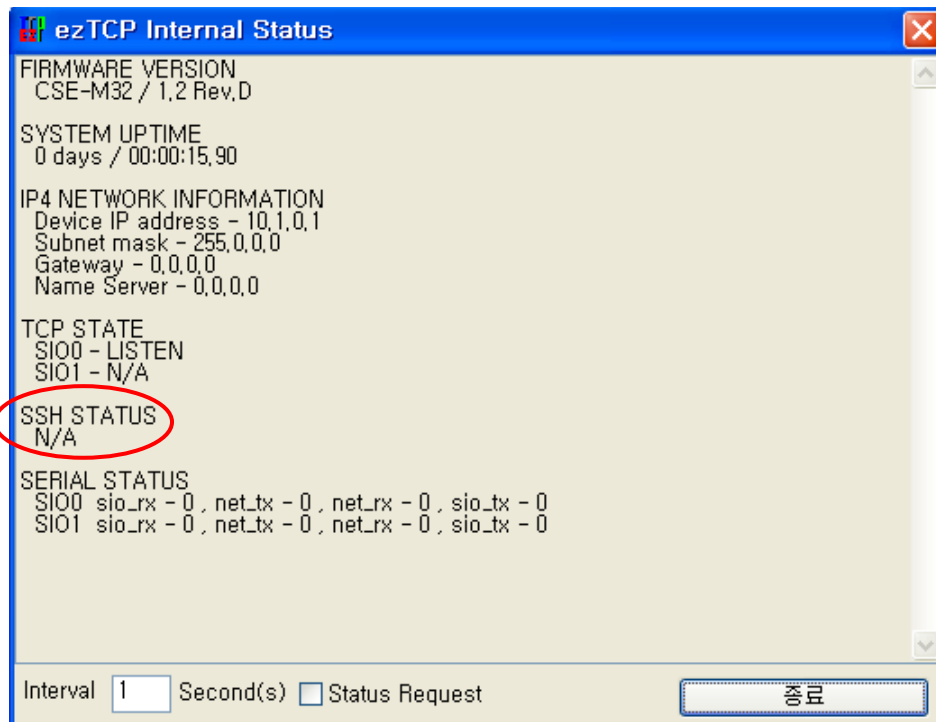
3 Example of use

This section describes how to communicate with ezTCP which is enabled "SSH" feature.

3.1 Confirm setting

3.1.1 Confirm setting with ezManager

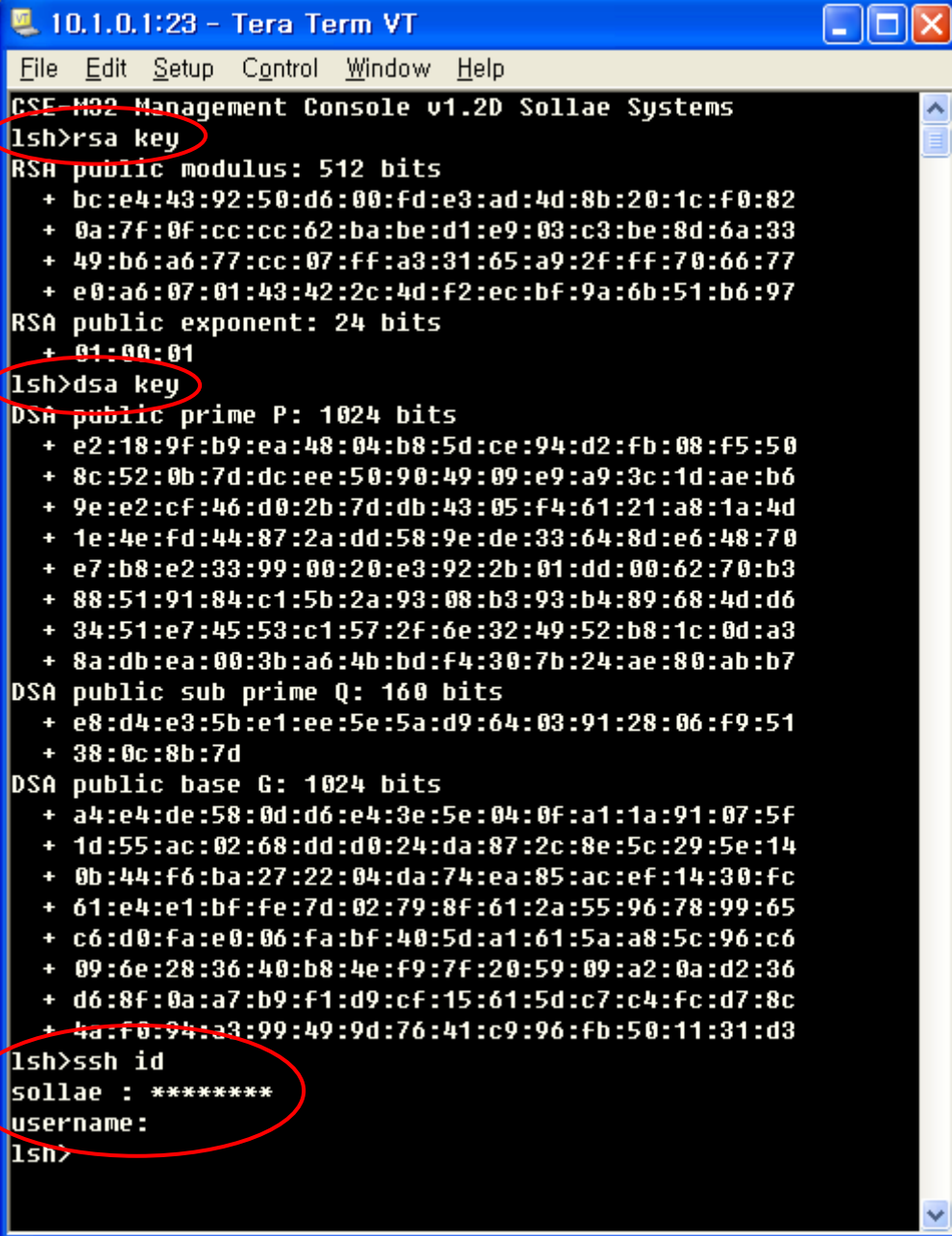
Click the [STATUS] button of ezManger.



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

3.1.2 Confirm setting with telnet console

After log in telnet console of ezTCP, check RSA KEY, DSA KEY and user ID/PW. The related command is "rsa key", "dsa key" and "ssh id". When user ID/PW lost, user can make new user ID/PW by "ssh id" command. After ezTCP receive "ssh id" command, ezTCP print currently user ID/PW (PW is printed in '*' symbols) and request new user ID. If user doesn't want to change currently user ID/PW, just type <Enter>. After changing user ID/PW, user must save the currently configuration by "ssh save aa55cc33" command.



```
10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
GSE M02 Management Console v1.2D Sollae Systems
1sh>rsa key
RSA public modulus: 512 bits
+ bc:e4:43:92:50:d6:00:fd:e3:ad:4d:8b:20:1c:f0:82
+ 0a:7f:0f:cc:cc:62:ba:be:d1:e9:03:c3:be:8d:6a:33
+ 49:b6:a6:77:cc:07:ff:a3:31:65:a9:2f:ff:70:66:77
+ e0:a6:07:01:43:42:2c:4d:f2:ec:bf:9a:6b:51:b6:97
RSA public exponent: 24 bits
+ 01:00:01
1sh>dsa key
DSA public prime P: 1024 bits
+ e2:18:9f:b9:ea:48:04:b8:5d:ce:94:d2:fb:08:f5:50
+ 8c:52:0b:7d:dc:ee:50:90:49:09:e9:a9:3c:1d:ae:b6
+ 9e:e2:cf:46:d0:2b:7d:db:43:05:f4:61:21:a8:1a:4d
+ 1e:4e:fd:44:87:2a:dd:58:9e:de:33:64:8d:e6:48:70
+ e7:b8:e2:33:99:00:20:e3:92:2b:01:dd:00:62:70:b3
+ 88:51:91:84:c1:5b:2a:93:08:b3:93:b4:89:68:4d:d6
+ 34:51:e7:45:53:c1:57:2f:6e:32:49:52:b8:1c:0d:a3
+ 8a:db:ea:00:3b:a6:4b:bd:f4:30:7b:24:ae:80:ab:b7
DSA public sub prime Q: 160 bits
+ e8:d4:e3:5b:e1:ee:5e:5a:d9:64:03:91:28:06:f9:51
+ 38:0c:8b:7d
DSA public base G: 1024 bits
+ a4:e4:de:58:0d:d6:e4:3e:5e:04:0f:a1:1a:91:07:5f
+ 1d:55:ac:02:68:dd:d0:24:da:87:2c:8e:5c:29:5e:14
+ 0b:44:f6:ba:27:22:04:da:74:ea:85:ac:ef:14:30:fc
+ 61:e4:e1:bf:fe:7d:02:79:8f:61:2a:55:96:78:99:65
+ c6:d0:fa:e0:06:fa:bf:40:5d:a1:61:5a:a8:5c:96:c6
+ 09:6e:28:36:40:b8:4e:f9:7f:20:59:09:a2:0a:d2:36
+ d6:8f:0a:a7:b9:f1:d9:cf:15:61:5d:c7:c4:fc:d7:8c
+ 4a:f0:94:a3:99:49:9d:76:41:c9:96:fb:50:11:31:d3
1sh>ssh id
sollae : *****
username:
1sh>
```

3.1.3 Connecting to the ezTCP

To communicate with the ezTCP enabled the SSH feature remote host must support SSH client operation. Confirm SSH feature by using "Putty, freeware" support SSH client.

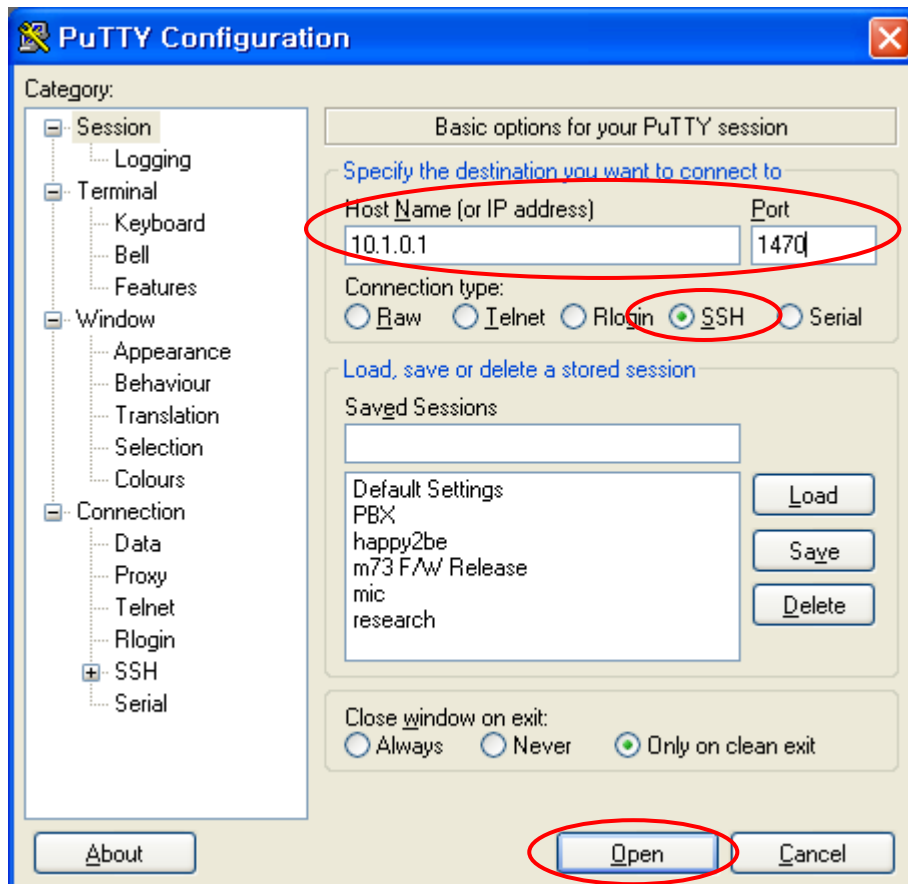
- Confirm basic parameter of ezTCP

Check the basic configuration of ezTCP as show below.

	PC	CSE-M32, CSE-H20, CSE-H21, CSE-M73, CSE-H25
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0
Local Port	-	1470
ezTCP Mode	-	T2S(0) – TCP Server

- Setting Putty

Set up the [Host Name] and [Port] respectively 'Local IP Address' and 'Local Port' of ezTCP as shown below.



Check the [Connection type] whether it is [SSH] then click [Open] button.

- Check KEY value of SSH Server(ezTCP)

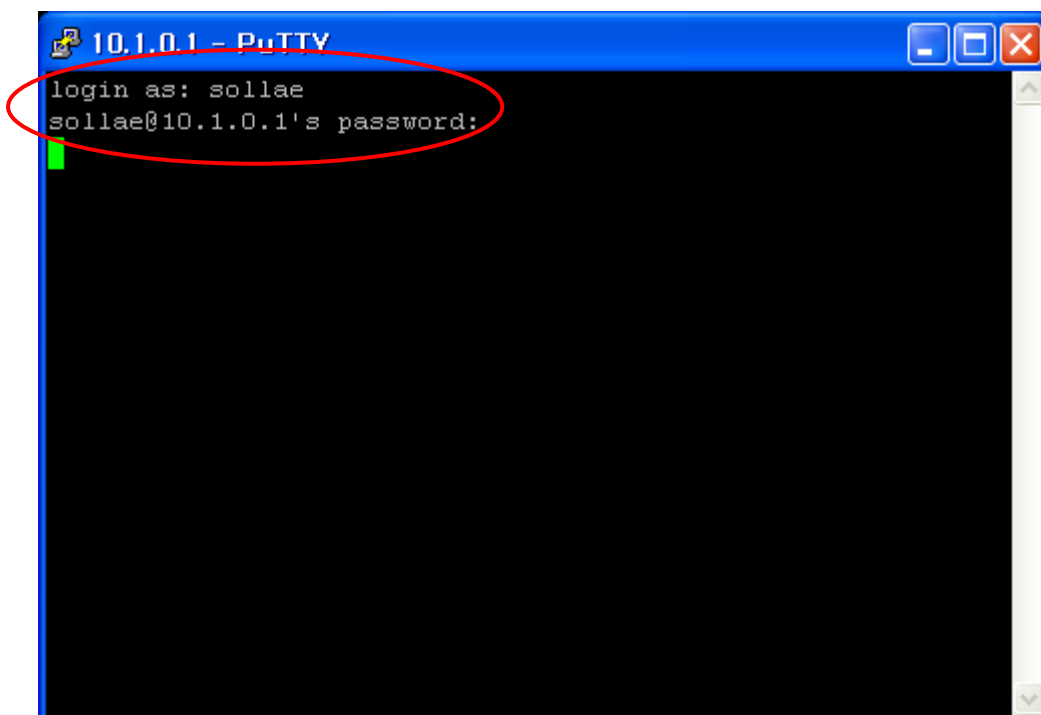
When user connect to ezTCP which is enabled "SSH" feature, pop up window like the below may appear.



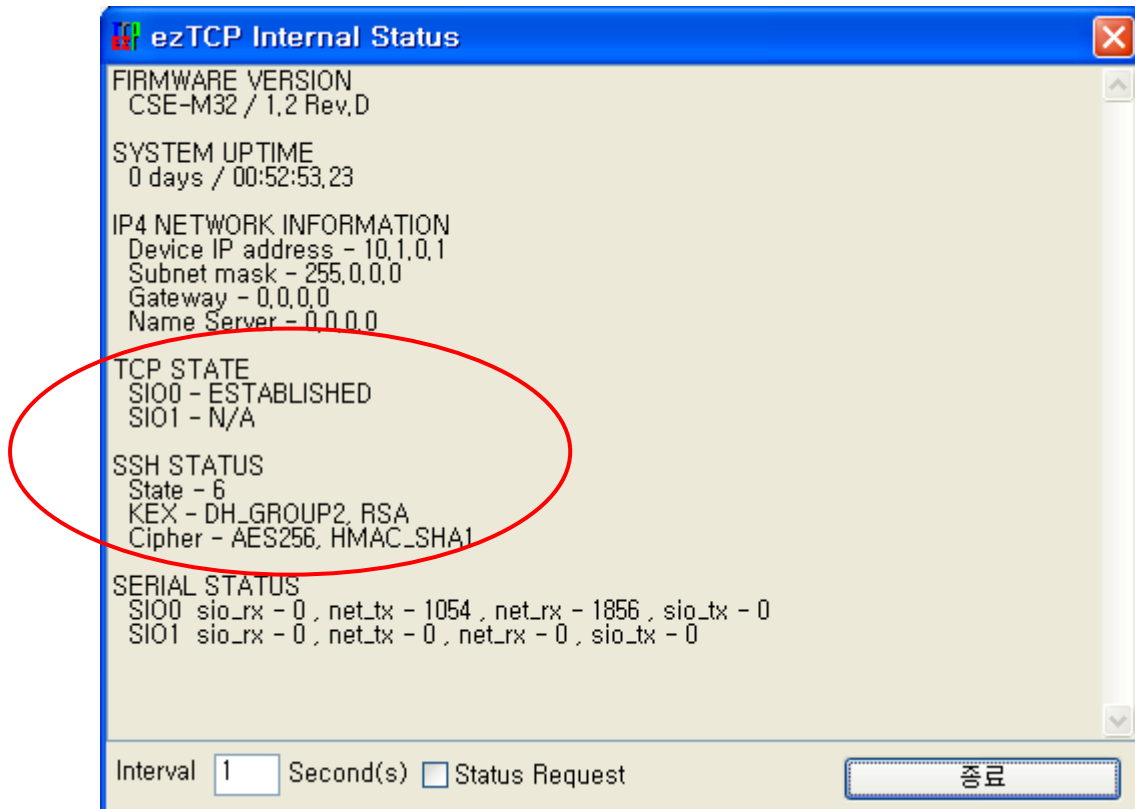
When and if the SSH server's key is not cached in SSH client, the SSH client ask whether it save the server's key. After saving the server's key once, the SSH client doesn't ask it again. If user change the key of ezTCP the SSH client will ask it again.

- Login

The below is first screen right after connect to the ezTCP. The ezTCP request user ID/PW, enter pre-configured ID and Password.



- Confirm TCP connection
Click the [STATUS] button of ezManager.



User can confirm "TCP STATE" / "SIO0 – ESTABLISHED" and "SSH STATUS" / "State – 6", "Cipher – AES_256, HMAC_SHA1".

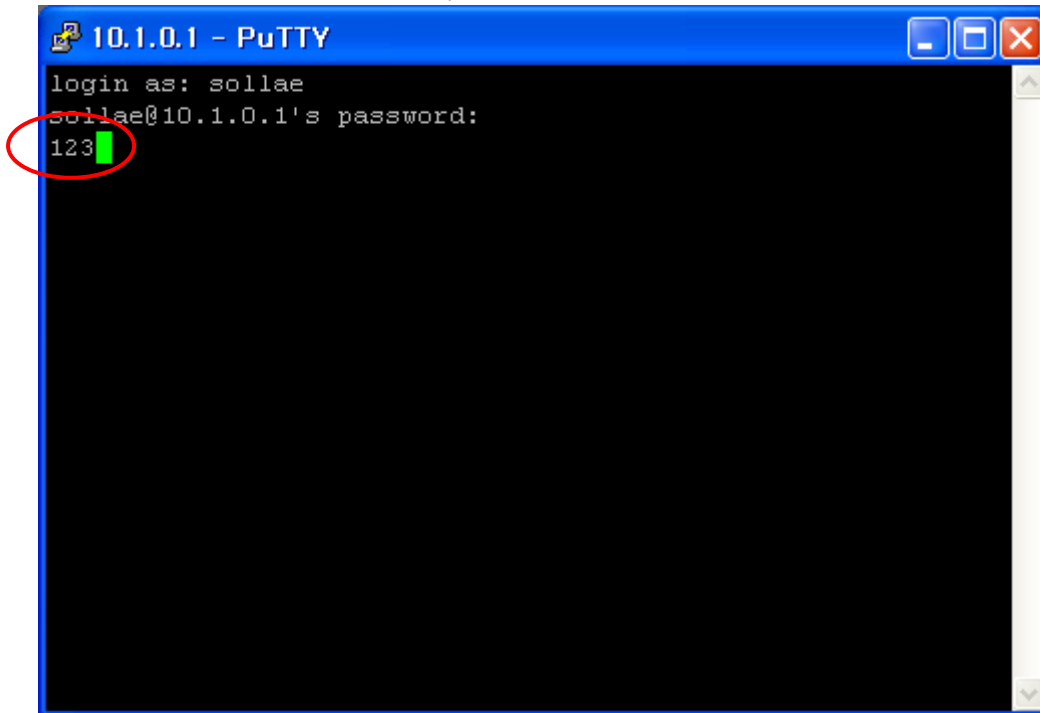
3.2 Communication test

After SSH connection succeeds, connect the serial port of PC to ezTCP's serial port. And check communication between client host PC and ezTCP.

Open serial port of PC and enter "123" on that Serial terminal, then this data-"123"- will appear on the Putty terminal. By contrast, enter "abc" on the Putty terminal and then this data- "abc"- will appear on the Serial terminal.

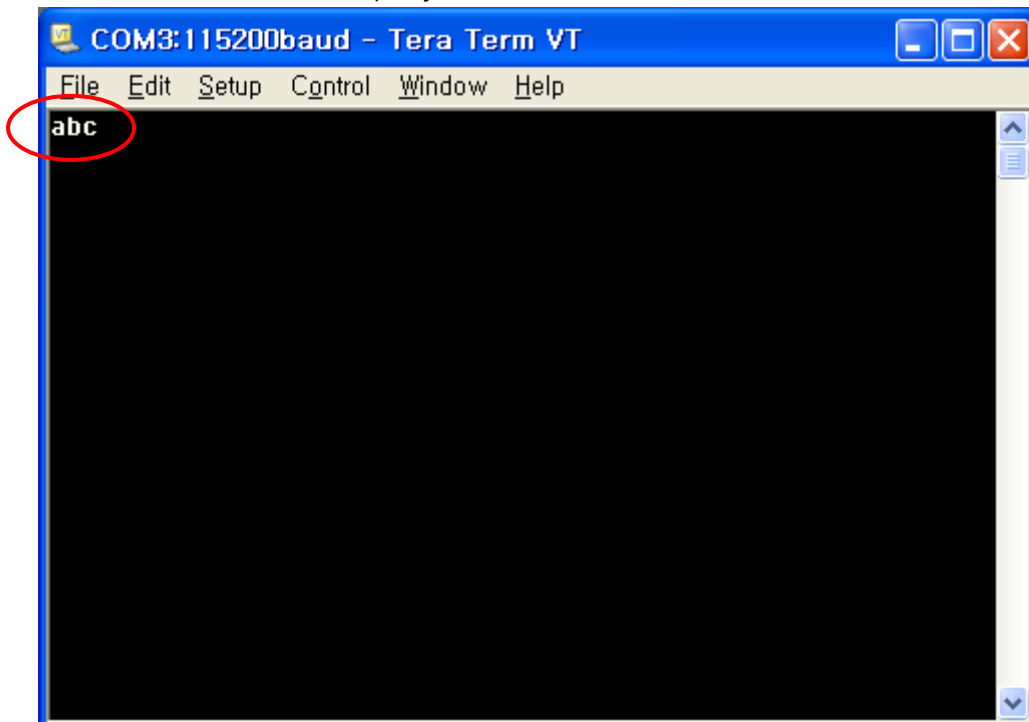
3.2.1 Putty terminal

Received data – "123" from serial port of ezTCP



3.2.2 Serial terminal

Received data – "abc" from putty terminal of client host



4 Revision History

Date	Version	Comments	Author
2008.10.23	1.0	○ Initial Release	-
2016.04.07	1.1	○ Add CSE-H25 on product list ○ Add an explanation about TELNET login	Roy LEE

