

Application Note

SSH (Secure Shell) - data

Version 1.0

2008-09-04

目录

1	概要	- 2 -
1.1	SSH (Secure Shell).....	- 2 -
1.2	ezTCP 应用.....	- 2 -
2	设定	- 3 -
2.1	设定前.....	- 3 -
2.2	设定SSH技能.....	- 3 -
2.2.1	激活SSH技能 -设定 ezManager.....	- 3 -
2.2.2	生成KEY.....	- 4 -
3	使用 例.....	- 7 -
3.1	通信 准备.....	- 7 -
3.1.1	ezManager 确认.....	- 7 -
3.1.2	telnet 连接确认.....	- 7 -
3.1.3	连接.....	- 8 -
3.2	通信试验.....	- 11 -
3.2.1	确认Putty端口.....	- 12 -
3.2.2	确认串口端.....	- 12 -
4	REVISION HISTORY	- 13 -

1 概要

1.1 SSH (Secure Shell)

SSH也称作Secure Socket Shell保证网络中，设备之间传输的数据通过安全的频率进行通信，为了安全进出远程电脑而制作的协议。目前广泛使用在维护因特网安全环境的协议，我公司产品支持SSH2版本。

1.2 ezTCP 应用

开始SSH是网络管理人员，为了远程控制各种设备，而代替现有的Telnet并生成的协议。现有的EZL串口产品（例：EZL-200F）已适应此要求并通过连接SSH代替Telnet，检测设备状态，设定环境变化值等。

此文件是为将串口端口以控制台使用的使用者设备，通过SSH保安协议登录并进行通信的说明，适应产品有CSE-M32, CSE-M73, CSE-H20, CSE-H21。

2 设定

2.1 设定前

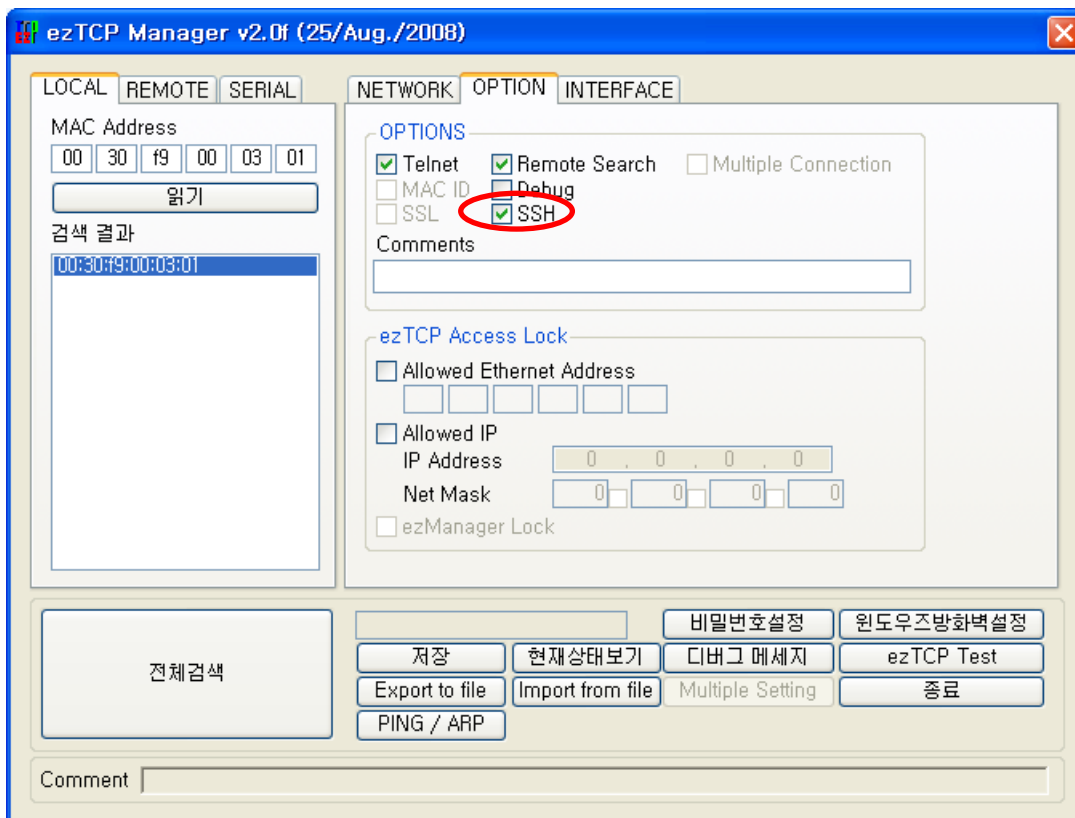
- 只能使用ezTCP Mode T2S(0) – TCP Server 模式。
- 使用SSH技能时，无法使用以下技能。
SSL, Telnet COM Port Control Option
- 使用SSH技能中各产品限制使用的事项如下。
CSE-M32, CSE-H20, CSE-H21 –无法使用COM2
CSE-M73 –无法使用远程控制技能

2.2 设定 SSH 技能

SSH只支持在TCP服务器模式。在服务器设置设定ezManager后连接Telnet，生成(参考2.2.2节) KEY后
可使用。

2.2.1 激活 SSH 技能 –设定 ezManager

按如下图所示设定[OPTION]栏中的[SSH]项目。

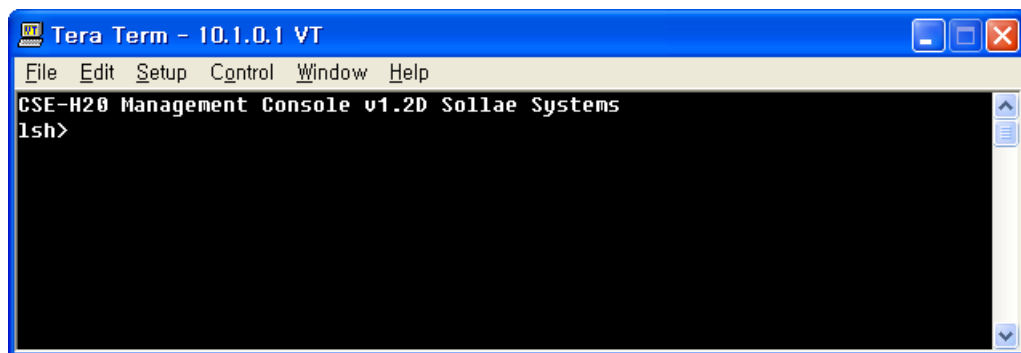


2.2.2 生成 KEY

- 与SSH有关的telnet命令如下。

项目	命令	说明
RSA KEY	rsa keygen <key length>	支援 KEY 长度 512/768/1024
	rsa key	确认已生成RSA KEY
	rsa test	测试已生成RSA KEY
DSA KEY	dsa keygen	生成RSA KEY后执行
	dsa key	确认已生成DSA KEY
ID/PW	ssh id	设定登录 ID / PW
保存设定	ssh save aa55cc33	保存有关SSH设定

- 连接ezTCP的超级终端。



- 生成RSA KEY

先生成RSA KEY。支援KEY的长度是512, 768, 1024 字节，按其容量大小可能生成数分钟，KEY的长度越长其需要的时间越长。1024字节的KEY平均生成时间需要1分钟。命令按此画面以

'rsa keygen <key length>'形式输入。

```

Tera Term - 10.1.0.1 VT
File Edit Setup Control Window Help
CSF-M20 Management Console v1.2D Sollae Systems
lsh>rsa keygen 1024
average 70000 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 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
401 406 409 412 416 421 428 442 443 446 449 458 467 479 482 497 509 511 523
524 537 541 544 551 559 566 577 584 586 587 593 598 616 632 638 644 found
rsa: RSA key pair(public/private key) generated.
rsa: key validation OK
lsh>

```

生成的RSA KEY可通过命令 'rsa test'可测试是否按正常形式生成的。
目前产品的RSA KEY可通过'rsa key'命令确认。

- DSA KEY 生成
如RSA KEY正常生成情况下，可通过'dsa keygen' 命令生成DSA KEY。

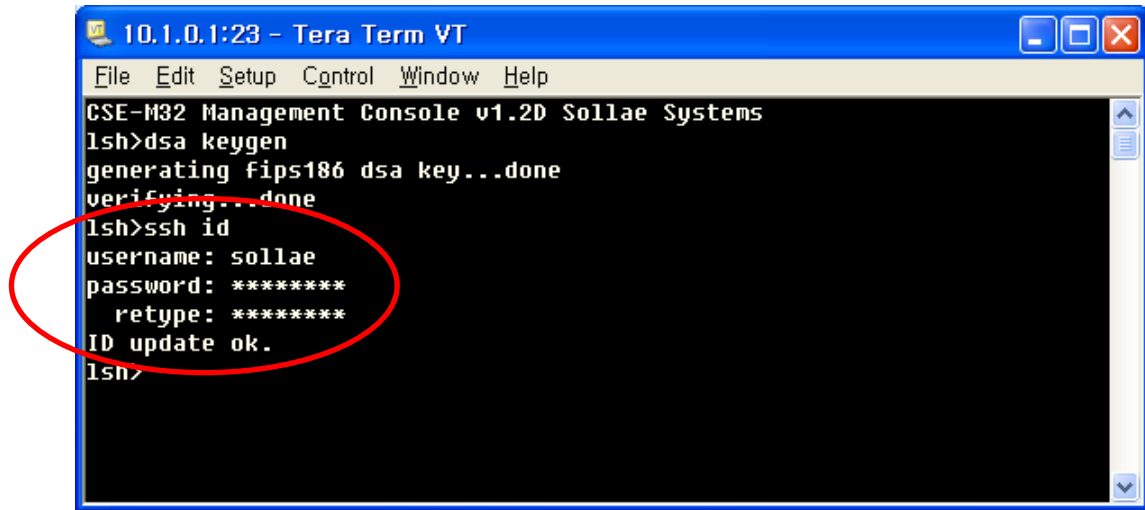
```

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>

```

目前生成的DSA KEY可通过'dsa key' 命令确认。

- 登录ID / PW 设定
为了登录SSH的ID及密码可通过'ssh id'命令设定。

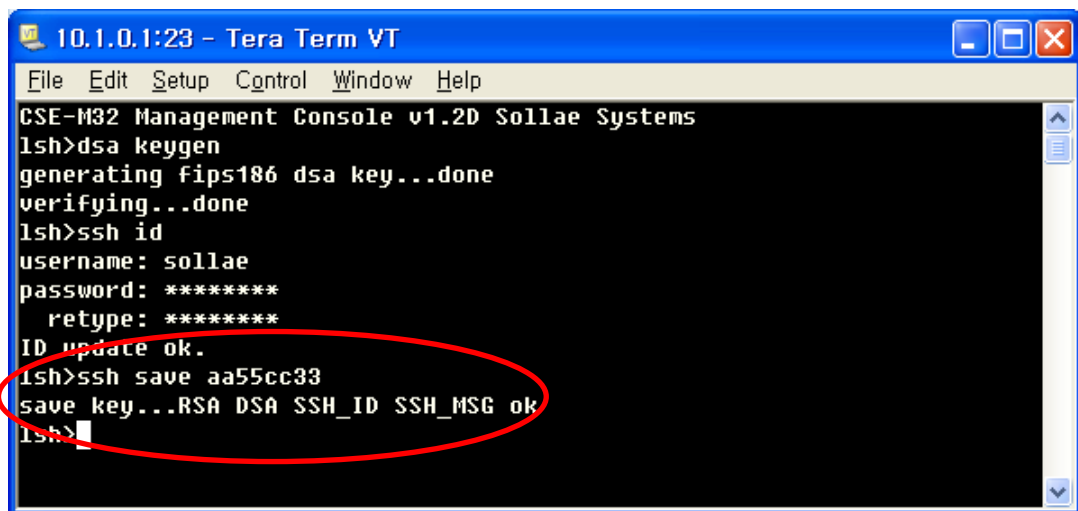


```

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>

```

- 设定项目
为了SSH保安通信生成的RSA KEY, DSA KEY与ID/PW需要储存在产品的非易失性存储器中。
'ssh save aa55cc33'为命令。



```

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>

```

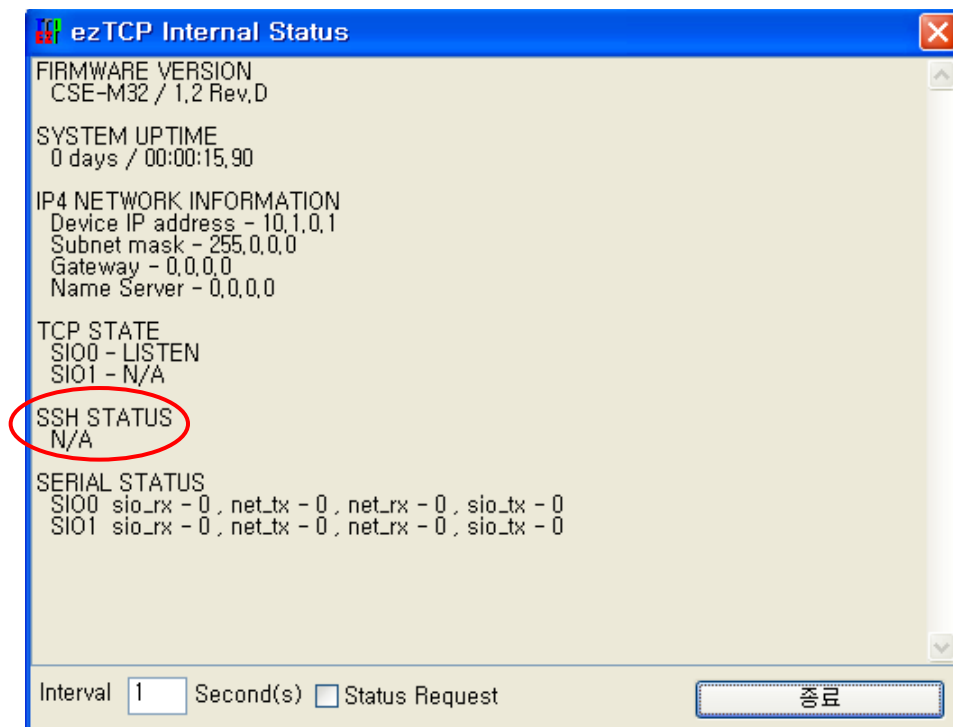
3 使用 例

在按SSH服务器动作的产品，通过输入SSH客户端程序设定的使用者ID与PW登录后与串口设备进行通信。

3.1 通信 准备

3.1.1 ezManager 确认

在ezManager按 [STATUS]按钮确认当前状态。



如上图 请确认是否出现SSH STATUS项目。

3.1.2 telnet 连接确认

连接产品的超级终端确认RSA KEY, DSA KEY与使用者的ID/PW。相关命令为 'rsa key', 'dsa key', 'ssh id'。输入'ssh id'命令将输出使用者的ID/PW (PW显示为'*)并要求新的使用者ID。此时输入回车键确认目前设定值后终止，如使用者丢失了ID/PW可以输入使用者的新ID/PW。输入新的使用者ID/PW后必须通过使用'ssh save aa55cc33'命令保存设置。


```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE M32 Management Console v1.20 Sollae Systems
lsh>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
lsh>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:a8:99:49:9d:76:41:c9:96:fb:50:11:31:d3
lsh>ssh id
sollae : *****
username:
lsh>

```

3.1.3 连接

要与已激活SSH技能的ezTCP进行通信，在对方HOST中需要有支持SSH的客户端。此章介绍的是利用商用免费SSH客户端Putty程序测试的过程。

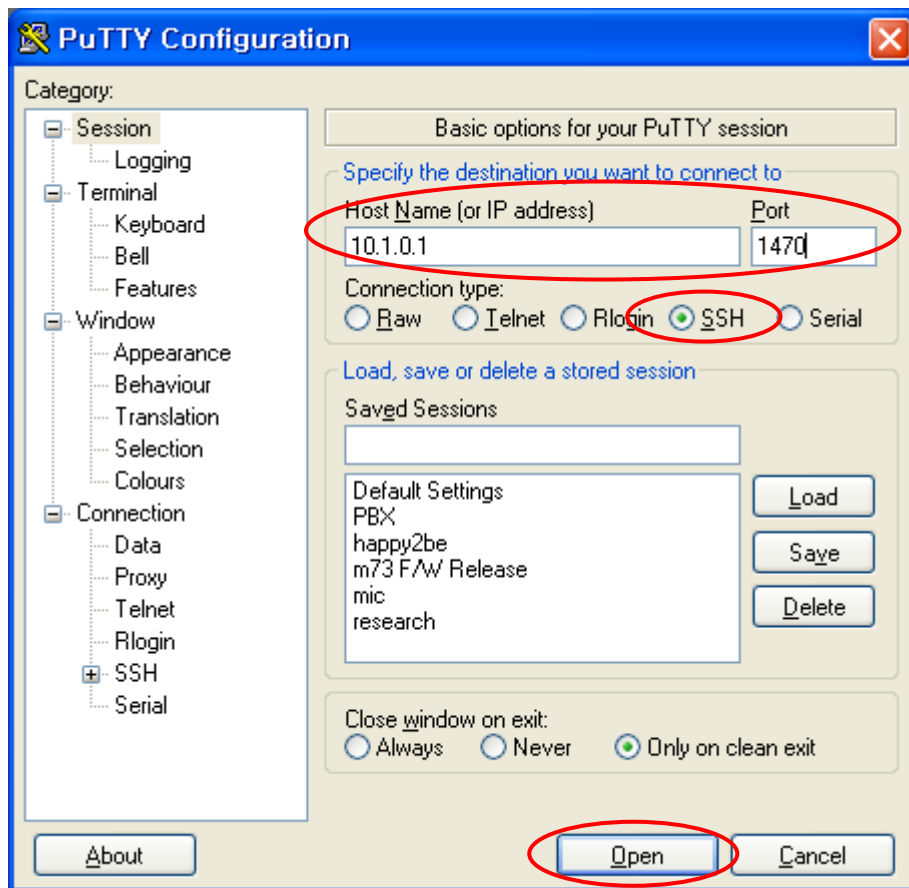
- 设定前确认事项

产品的IP地址与Port号码需要正确设置为符合设置ezTCP的环境。为了帮助理解，产品的IP假设为出厂值并确认设定事项。

	PC	CSE-M32, CSE-H20, CSE-H21, CSE-M73
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0
Local Port	-	1470

- Putty设定事项

如在下面Putty的初始画面标示的部分，请输入ezTCP产品的Local IP Address与Local Port 号码。



输入后如上图所示确认是否为Connection type的SSH后接Open按钮。

- 确认服务器KEY

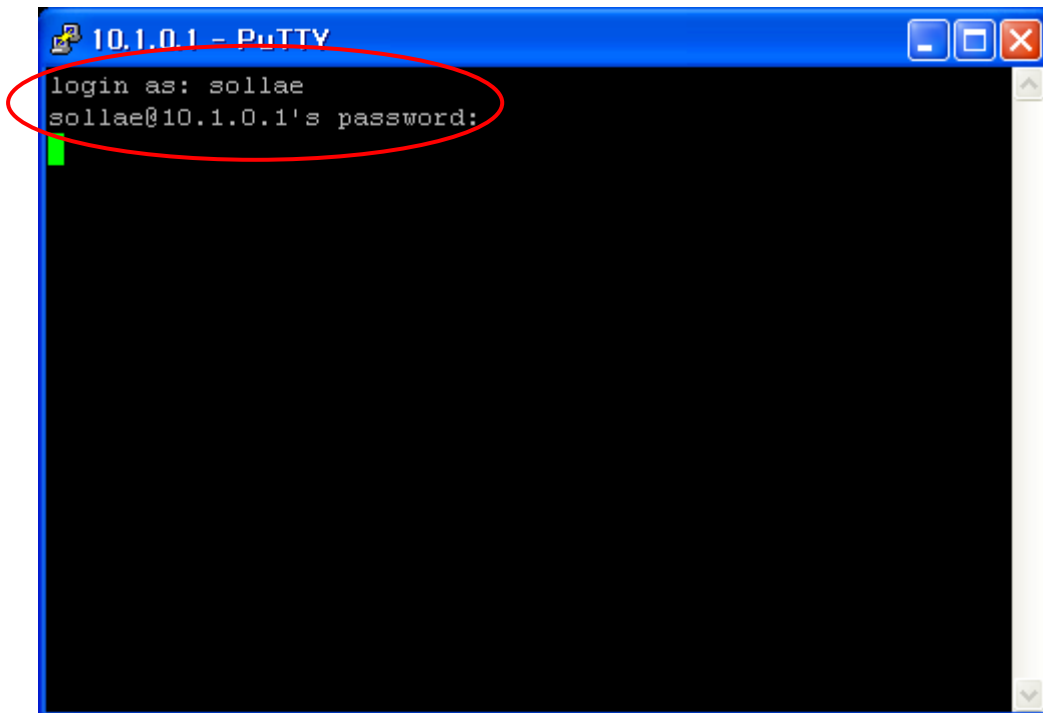
激活ezTCP产品的SSH技能后，初次连接时出现如下画面。



此为初次连接并储存ezTCP产品KEY情报值时出现，请按‘是(Y)’按钮后进行到下一阶段。只要保存一次，下次出现不会再问是否保存与否。但更改ezTCP的KEY值后最初连接时需要保存KEY值。

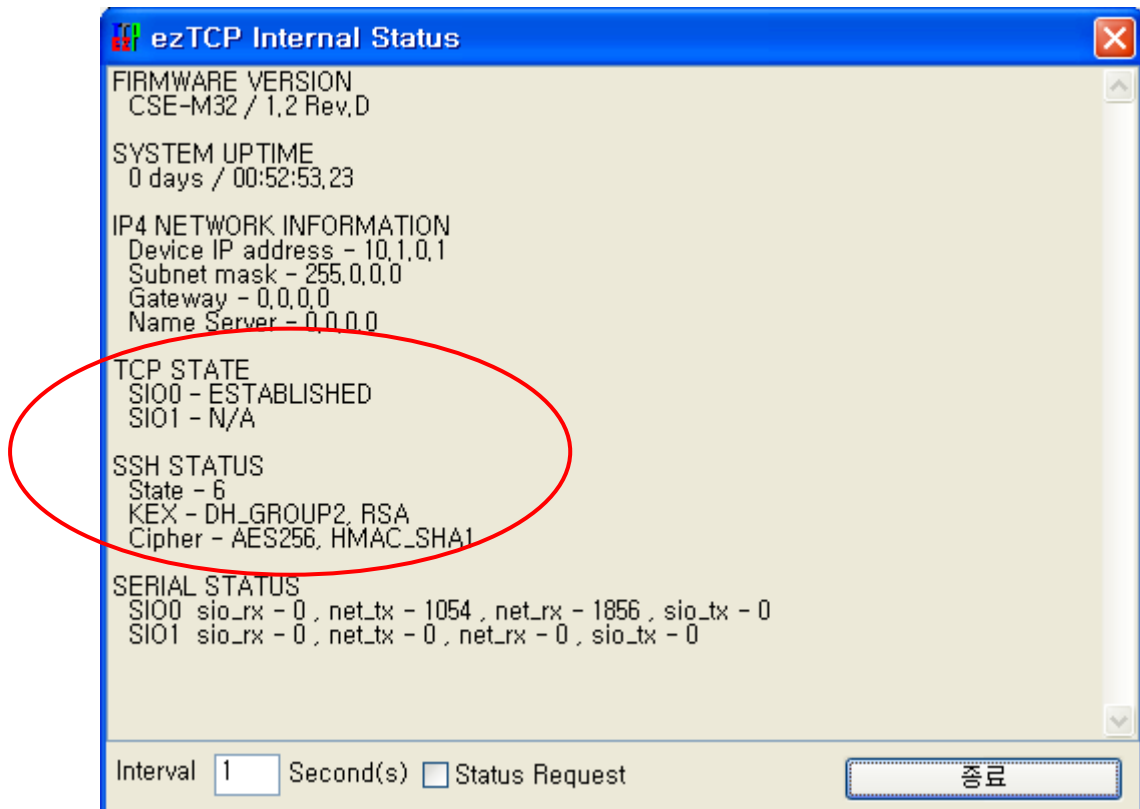
- 登录

下面是登录后第一个画面。此时要求输入之前设定的ID/PW，请按顺序输入。



- 确认TCP连接

在ezManager按[STATUS]按钮，查看目前状态。



如上图在TCP STATE项目中出现[SIO0 – ESTABLISHED], 出现SSH STATUS 项目的 [State – 6], [Cipher – AES_256, HMAC_SHA1] 可确认为已做好通信准备。

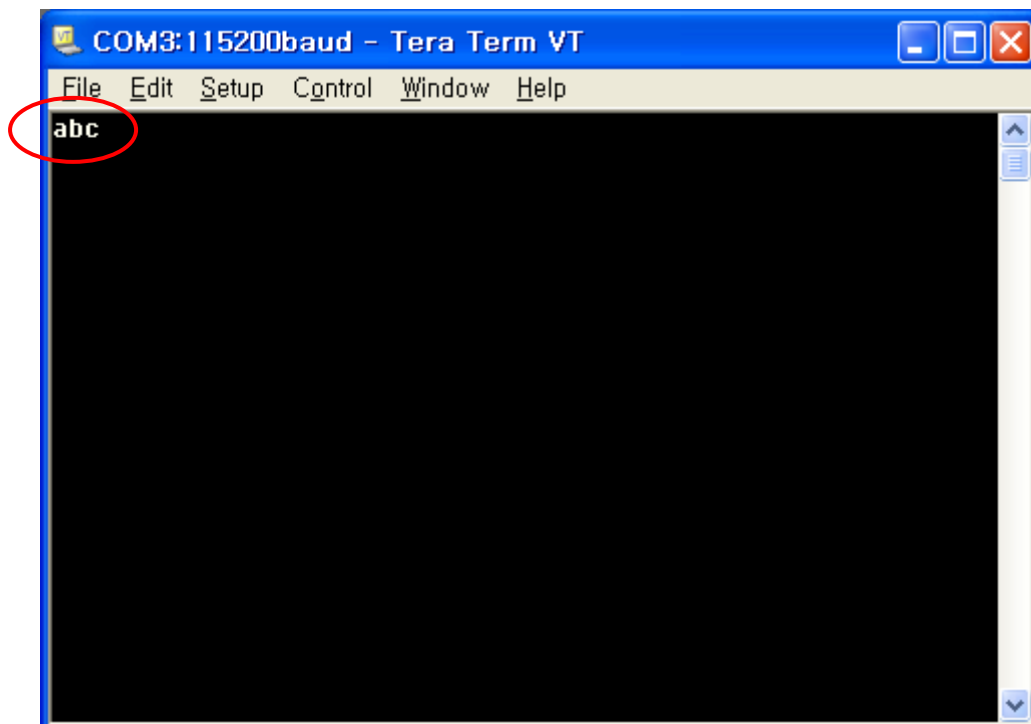
3.2 通信试验

连接SSH后, 开放ezTCP产品的串口端口并确认是否有往来的数据。在串口端窗口输入“123”, 在Putty窗显示“123”, 相反在Putty端窗口输入“abc”, 在串口端出现“abc”。此时, 往来的数据已经是通过加密后送接收的, 不同于一般通信模式下适用于保安要求严格的环境下。

3.2.1 确认 Putty 端口



3.2.2 确认串口端



4 Revision History

Date	Version	Comments
Sep. 04. 2008	1.0	Initial Release