

Application Note

# SSL (Secure Socket Layer)

Version 1.1  
2009-06-11

## 目录

<b>1</b>	<b>概要</b> .....	<b>- 2 -</b>
1.1	SSL (Secure Socket Layer).....	- 2 -
1.2	适用 .....	- 2 -
<b>2</b>	<b>设定</b> .....	<b>- 3 -</b>
2.1	设定之前.....	- 3 -
2.2	设定 .....	- 3 -
2.2.1	概要.....	- 3 -
2.2.2	ezManager 设定.....	- 3 -
2.2.3	生成证书.....	- 4 -
<b>3</b>	<b>使用例</b> .....	<b>- 9 -</b>
3.1	概要 .....	- 9 -
3.1.1	连接TCP状态 .....	- 9 -
3.2	TCP 服务器模式.....	- 9 -
3.2.1	ezManager 确认 .....	- 9 -
3.2.2	确认Telnet连接.....	- 10 -
3.2.3	连接.....	- 11 -
3.3	TCP客户端模式.....	- 14 -
<b>4</b>	<b>REVISION HISTORY</b> .....	<b>- 15 -</b>

# 1 概要

## 1.1 SSL (Secure Socket Layer)

SSL最初是为了电子商务保安由 Netscape公司开发的，后依据开发因特网标准规定的美国 IAB (Internet Architecture Board)的调查委员会 IETF (Internet Engineering Task Force)改为 TLS (Transport Layer Security)的标准名称。是目前广泛使用在维持因特网保安的协议，我公司产品支援 SSL 3.0 / TLS 1.0，确保在因特网环境下安全传送数据。

## 1.2 适用

因SSL在TCP上层动作故无法在U2S模式下使用UDP。此文是关于SSL在TCP服务器/客户端各模式下使用的应用文，适用产品是CSE-M32, CSE-M73, CSE-H20, CSE-H21,CSE-H25。

## 2 设定

### 2.1 设定之前

- 无法在 “U2S- UDP ”模式下使用。
- 使用SSL技能时无法使用如下技能。  
SSH保安通信,串口端口设定/状态传送 (RFC 2217)
- 使用SSL技能中各产品制约事项如下。  
CSE-M32, CSE-H20, CSE-H21 – 最高 串口通信速度为115,200bps / 无法使用COM2  
CSE-M73 – 最高串口通信速度115,200bps, 无法使用远程控制技能  
CSE-H25 – 串口通信速度最高115,200bps

### 2.2 设定

#### 2.2.1 概要

SSL技能可以分别在TCP服务器/客户端各自使用。在客户端模式单纯的激活“SSL 保安通信” (“2.2.2 ezManager 设定”)即可使用。在TCP服务器模式激活“SSL 保安通信”后连接Telnet并生成 (“2.2.3 生成证书”) 认证书后可使用。

- TCP 客户端  
“COD – TCP 客户端” 通信模式或是 “ATC – AT命令” 通信模式中通过“atd(t)”命令连接TCP
- TCP 服务器  
“T2S – TCP 服务器” 通信模式

SSL技能可以分别在TCP服务器/客户端各自使用。客户端模式(COD(2)模式或ATC(1)模式中使用‘atd’命令)时。只有通过ezManager激活(参考2.2.1节) SSL选项使用。

#### 2.2.2 ezManager 设定

按图2-1 在[OPTION] 栏中设定[SSL 保安通信]项目。

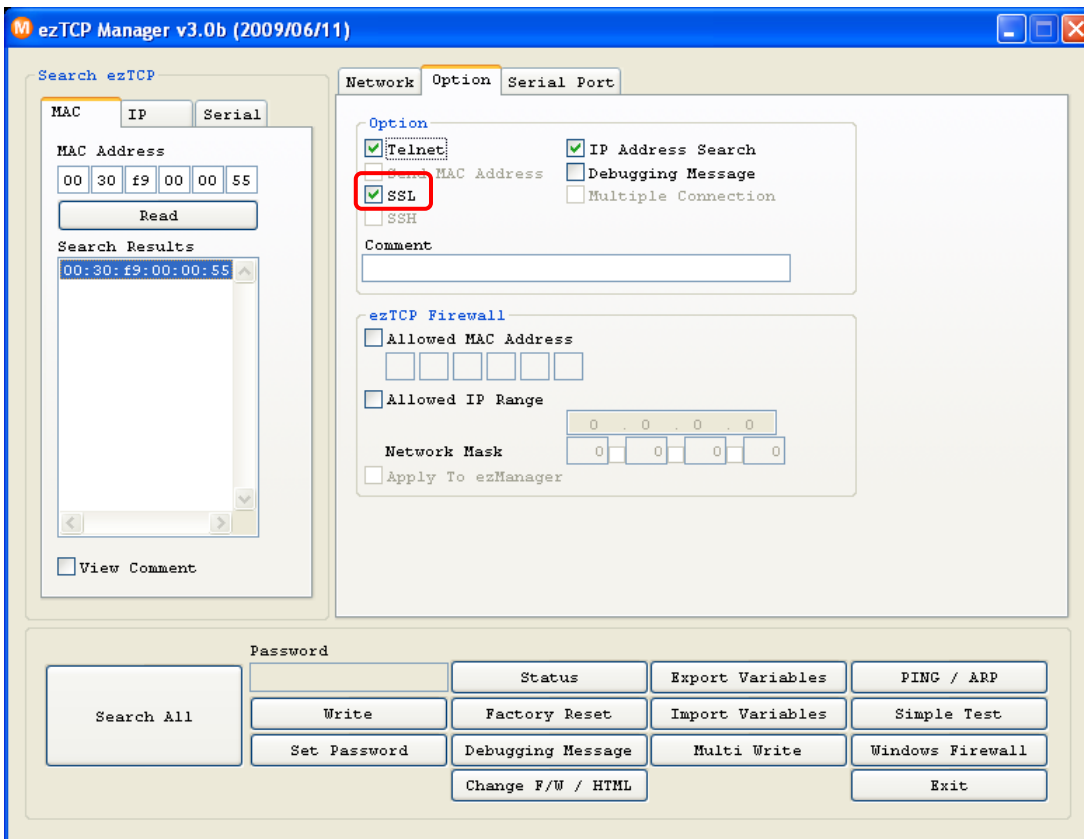


图 2-1 设定“SSL 保安通信”选项

### 2.2.3 生成证书

- 连接到产品 (ezTCP) 的 Telnet。

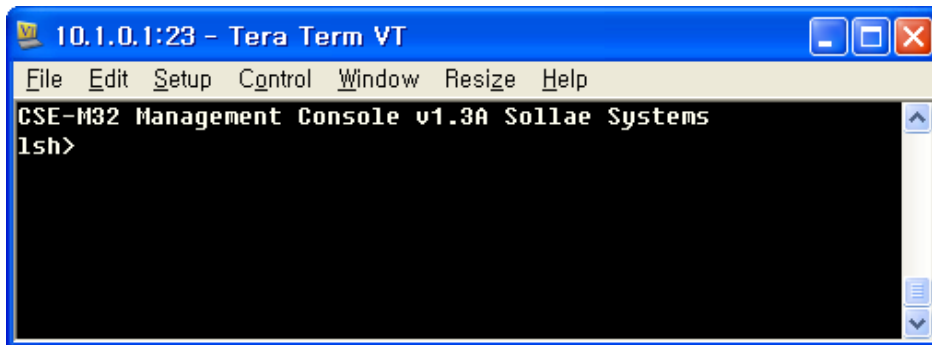


图 2-2 连接 Telnet

- 与SSL相关的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	确认生成的 RSA KEY
	rsa test	测试生成的 RSA KEY
认证书	cert new	已生成利用RSA KEY认证书
	cert view	确认目前认证书
储存设定	ssl save aa55cc33	储存有关SSL关联设定

表 2-1 SSL 技能说明 命令

- 生成RSA KEY

为了生成认证书先生成RSA KEY。支援KEY长度是512, 768, 1024 字节，生成时根据长度需要数分钟，KEY的长度越长时间也跟着变长。1024字节的KEY平均需要1分钟左右。命令形式按如下画面按'rsa keygen <key length>'形式输入。下面是实际使用例子。

```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Resize Help
CSE-M32 management console v1.3A Sollae Systems
lsh>rsa keygen 1024
average 50sec required to find two 512bits prime numbers, please wait..
rsa: find 512bits random prime p..0 1 2 5 8 11 16 20 23 26 31 38 43 46 47 5
2 53 65 68 76 85 88 92 97 101 106 107 115 125 136 142 146 148 155 157 158 1
63 167 172 173 190 205 223 232 241 250 251 260 262 271 272 275 286 293 296
307 311 320 323 326 328 332 337 340 353 361 365 368 370 376 382 398 400 401
403 407 416 418 422 430 431 433 437 442 452 458 460 463 506 515 530 533 53
5 536 547 548 550 557 562 575 577 586 590 601 605 608 617 626 628 632 638 6
40 652 691 727 731 733 736 745 748 758 766 782 788 790 796 803 806 817 823
832 838 845 860 871 877 878 881 890 892 895 898 905 913 920 925 935 947 953
968 992 1000 1003 1012 1013 1028 1033 1045 1061 1066 1076 1081 1082 1087 1
091 1097 1100 1105 1121 1132 1135 1136 1138 1142 1147 1165 1180 1196 1208 1
210 1213 1217 1228 1237 1240 1247 1258 1261 1268 1276 1277 1285 1297 1298 1
300 1306 1310 1331 1342 1345 1346 1355 1360 1367 1373 1382 1385 found
rsa: find 512bits random prime q..1 3 4 9 12 16 19 24 31 36 39 42 43 46 49
57 58 61 63 66 67 78 81 82 88 93 108 124 127 136 144 154 159 162 163 169 18
4 189 196 213 214 219 222 226 231 234 246 247 253 256 259 261 273 276 289 2
92 297 303 306 312 313 316 318 324 331 352 358 361 364 366 367 379 387 388
393 396 408 418 427 438 441 451 462 466 472 474 found
rsa: RSA key pair(public/private key) generated.
rsa: key validation OK
rsa: rsa_server_key exist, replaced to new key
lsh>

```

图 2-3 生成RSA KEY

生成的RSA KEY可根据'rsa test' 命令可测试目前是否按正常动作，目前产品的RSA KEY可通过'rsa key' 命令进行确认。

☞ 生成RSA KEY时原来的RSA KEY自动更换为新的。

- 生成认证书  
正常生成RSA KEY后通过'cert new' 命令生成认证书。

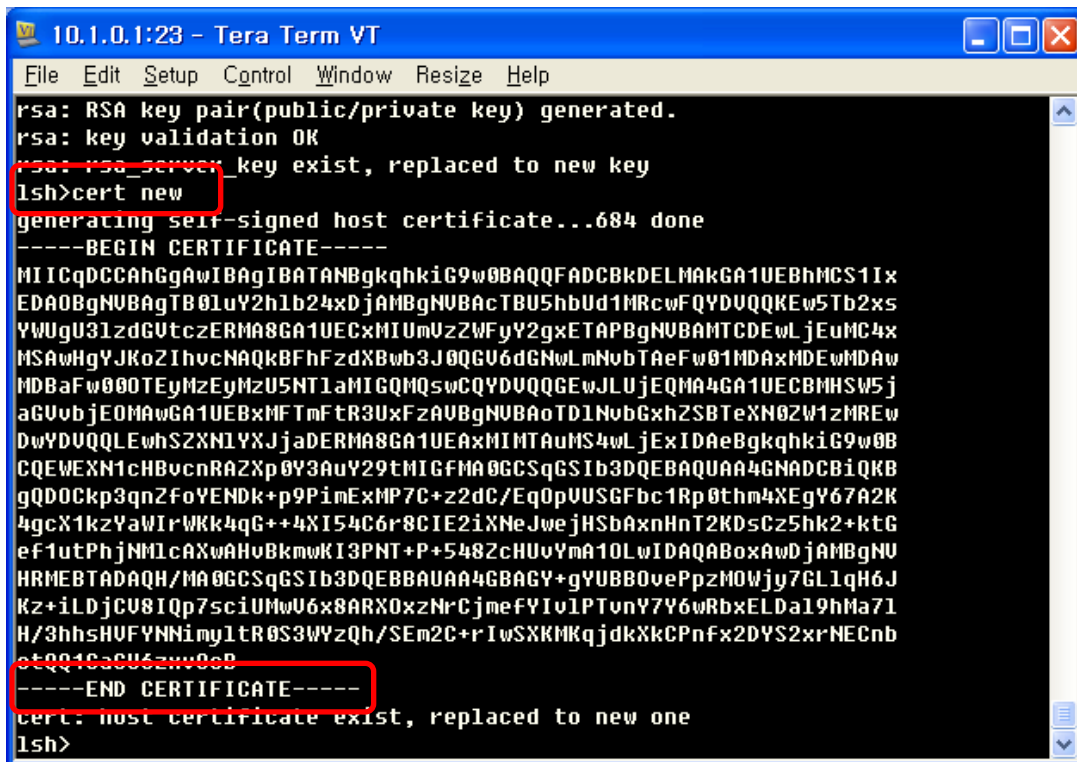


图 2-4 生成证书

不同于不需要证书的SSL客户端，SSL服务器需要持有证书。在上过程中生成的产品(ezTCP)是包含自身的IP情报的自发证书。故产品的IP地址每发生变化时请重新生成新的证书。

*生成证书原来的证书自动更换为新生成的证书。*

- 储存设定事项  
 为了SSL保安通信，需将生成的RSA KEY与证书储存在非易失性存储器中。命令是'ssl save aa55cc33'。



```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Resize Help
rsa: rsa_server_key exist, replaced to new key
lsh>cert new
generating self-signed host certificate...684 done
-----BEGIN CERTIFICATE-----
MIICqDCCAhGgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBkDELMAkGA1UEBhMCS1x
EDA0BgNUBAGTB0luY2h1b24xDjAMBgNUBACIBU5hbUd1MRcwFQYDUQKKEw5Tb2xs
YWUgU31zdGVtczERMA8GA1UECzMlUmVzZWZlY2gxEtAPBgNUBAMTCDEwLjEuMC4x
MSAwHgYJKoZIhvcNAQkBFhFzdXBwb3J0QG96dGNwLmNvbTAEFw01MDAxMDEwMDAw
MDBaFw000TEyMzU5NT1aMIGQMQswCQYDUQKKEwJLUjEQA4GA1UECBMhSW5j
aG9vbG90MAwGA1UEBxMFTmFtR3UxZmFzYU90bG90bG90bG90bG90bG90bG90bG90
DwYDUQKLEwhS2XN1YXJjaDERMA8GA1UEAxMlMlTmFtMS4wLjEwIDAeBgkqhkiG9w0B
CQEWEXN1cHBvcnRAZ2p0Y3AuY29tMIGFMA0GCQSqGSIB3DQEBAQUAA4GNADCBiQKB
gQD0Ckp3qnZfoYENDk+p9PimExMP7C+z2dC/Eq0pUUSGFbc1Rp0thm4XEgY67A2K
4gcX1kzYaWIrWkK4qG++4XI54C6r8CIE2ixNeJwejHSbAxnHnT2KDsCz5hk2+ktG
ef1utPhjNMLcAXwAHuBkmwKI3PNT+P+548ZcHUvYmA10LwIDAQABoxAwDjAMBGNu
HRMEBTADAQH/MA0GCQSqGSIB3DQEBAQUAA4GBAGY+gYUBBOvePpzMOWjy7GL1qH6J
Kz+iLDjCU8IQp7sciUMwU6x8ARX0xzNrCjmeFYIv1PTvnY7Y6wRbxELDa19hMa71
H/3hhsHUFYNNimy1tR0S3WYzQh/SEm2C+rIwSXKMKqjdkXkCPnfX2DYS2xrNECnb
otQQ1CaCU6zxv0cB
-----END CERTIFICATE-----
cert: host certificate exist, replaced to new one
lsh>ssl save aa55cc33
save key...RSA CERT_host ok
lsh>

```

图 2-4 设定SSL储存

## 3 使用 例

### 3.1 概要

#### 3.1.1 连接 TCP 状态

使用例子大范围可分为TCP服务器/客户端两部分，各各不同的ezTCP动作模式如下。

- TCP 服务器
  - “T2S – TCP服务器 ” 通信模式
  - “ATC – AT 命令” 模式下通过‘ata’命令的手动TCP连接
- TCP 客户端
  - “COD – TCP 客户端” 通信模式
  - “ATC – AT 命令”模式下通过‘atd(t)’命令的自动TCP连接

### 3.2 TCP 服务器模式

#### 3.2.1 ezManager 确认

在ezManager按[STATUS]按钮确认目前状态。

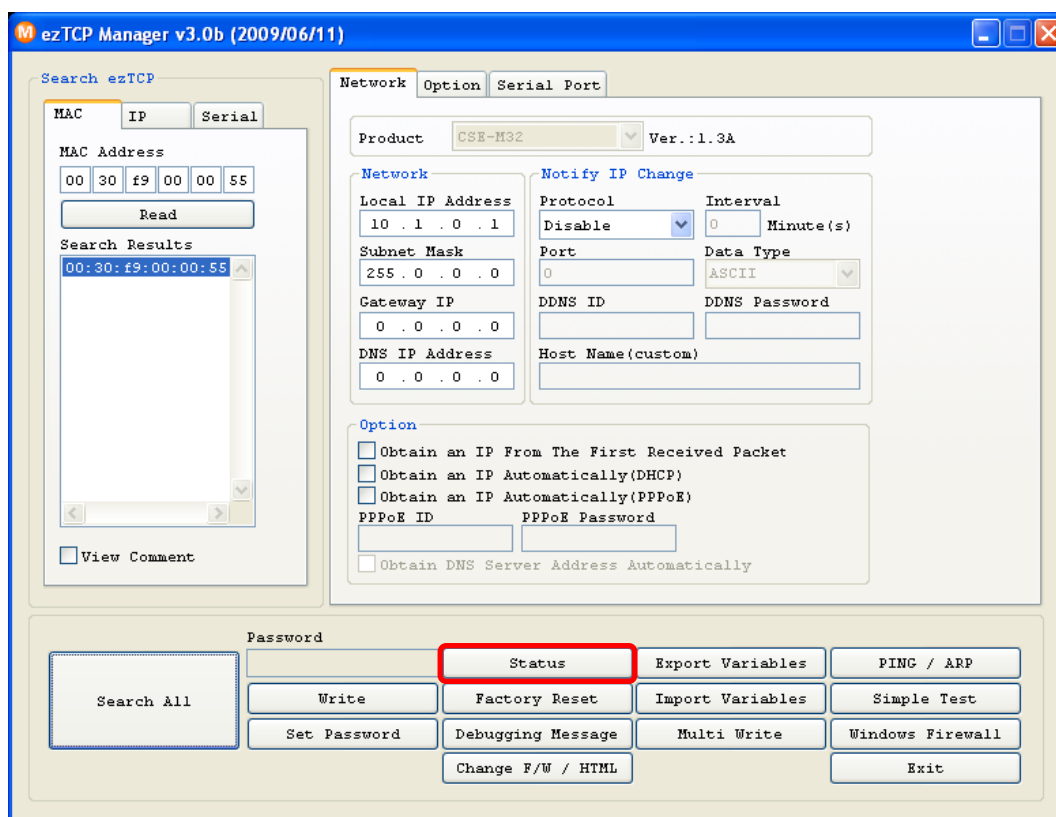


图 3-1 ezManager [STATUS] 按钮

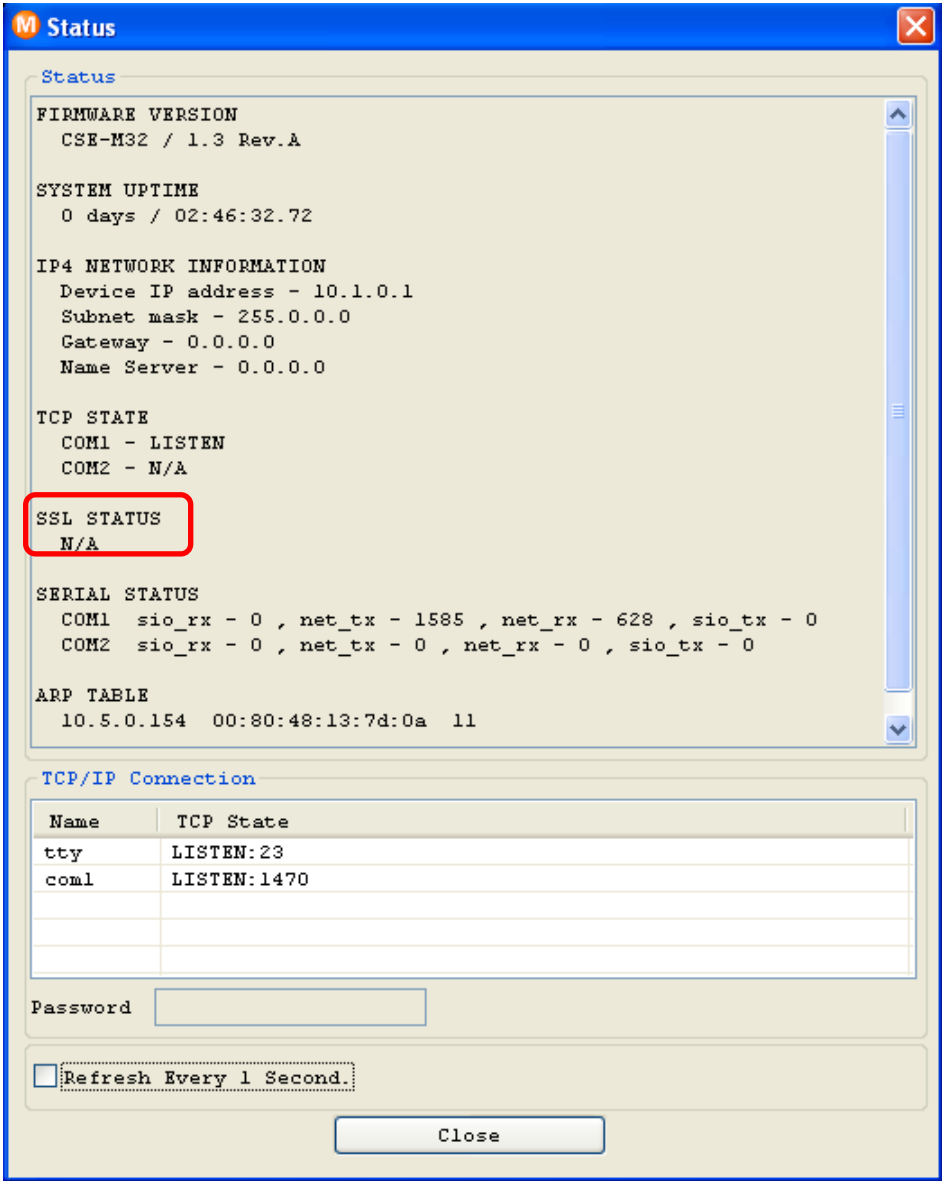


图 3-2 ezManager "STATUS" 画面

如上图确认是否显示SSL STATUS项目。

### 3.2.2 确认 Telnet 连接

连接产品的TELNET确认RSA KEY与认证生成。相关命令是'rsa key', 'cert view'。此时请确认证的IP与目前产品中设定的IP是否一致。

```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Resize Help
GSE-M32 Management Console v1.3A Sollae Systems
lsh>rsa key
RSA public modulus: 1024 bits
+ ce:0a:4a:77:aa:76:5f:a1:81:0d:0e:4f:a9:f4:f8:a6
+ 13:13:0f:ec:2f:b3:d9:d0:bf:12:a3:a9:55:44:86:15
+ b7:35:46:9d:2d:86:6e:17:12:06:3a:ec:0d:8a:e2:07
+ 17:d6:4c:d8:69:62:2b:58:a9:38:a8:6f:be:e1:72:39
+ e0:2e:ab:f0:22:04:da:25:cd:78:9c:1e:8c:74:9b:03
+ 19:c7:9d:3d:8a:0e:c0:b3:e6:19:36:fa:4b:46:79:fd
+ 6e:b4:f8:63:34:c9:5c:01:7c:00:1e:f0:64:9b:02:88
+ dc:f3:53:f8:ff:b9:e3:c6:5c:1d:4b:d8:98:0d:4e:2f
RSA public exponent: 24 bits
+ 01:00:01
lsh>cert view
ssl: + Issuer
ssl: + country / KR
ssl: + state or province / Incheon
ssl: + locality / NamGu
ssl: + organization / Sollae Systems
ssl: + organizationUnit / Research
ssl: + common / 10.1.0.1
ssl: + email / support@eztcp.com
ssl: + Validity
ssl: + notAfter 500101000000Z
ssl: + notBefore 491231235959Z
ssl: + Subject
ssl: + country / KR
ssl: + state or province / Incheon
ssl: + locality / NamGu
ssl: + organization / Sollae Systems
ssl: + organizationUnit / Research
ssl: + common / 10.1.0.1
ssl: + email / support@eztcp.com
ssl: + Public key OID: 1.2.840.113549.1.1.1. PKCS #1 RSA
ssl: + Extension OID: 2.5.29.19.
ssl: + 30:03:01:01:ff
ssl: + Signature Algorithm OID: 1.2.840.113549.1.1.4. md5WithRSA
Encryption
lsh>

```

图 3-3 RSA KEY 及确认证书

### 3.2.3 连接

如要与激活SSL技能的产品（ezTCP）进行通信，对方的HOST也要支持SSL。在本章节介绍通过我社ezVSP连接的测试过程。

- 设定前需要确认的事项  
产品的IP地址(“网络”栏中 [产品 IP地址] 及与“串口端口”栏中[进行通信的地址])与端口号码(“串口端口”栏中的 [产品本地地址]及 [进行通信的端口]) 需要设置为符合设置产品（ezTC

P) 的环境。但为了帮助理解将产品的IP地址设置为出厂值，并确认设定事项。

	产品(ezTCP)	PC
Local IP Address	10.1.0.1	10.1.0.2
Subnet Mask	255.0.0.0	255.0.0.0
产品本地端口	1470	-

表 3-1 确定设定值

- ezVSP 设定事项

请按ezManager的“串口端口”栏中的 [在生成ezVSP端口]按钮。

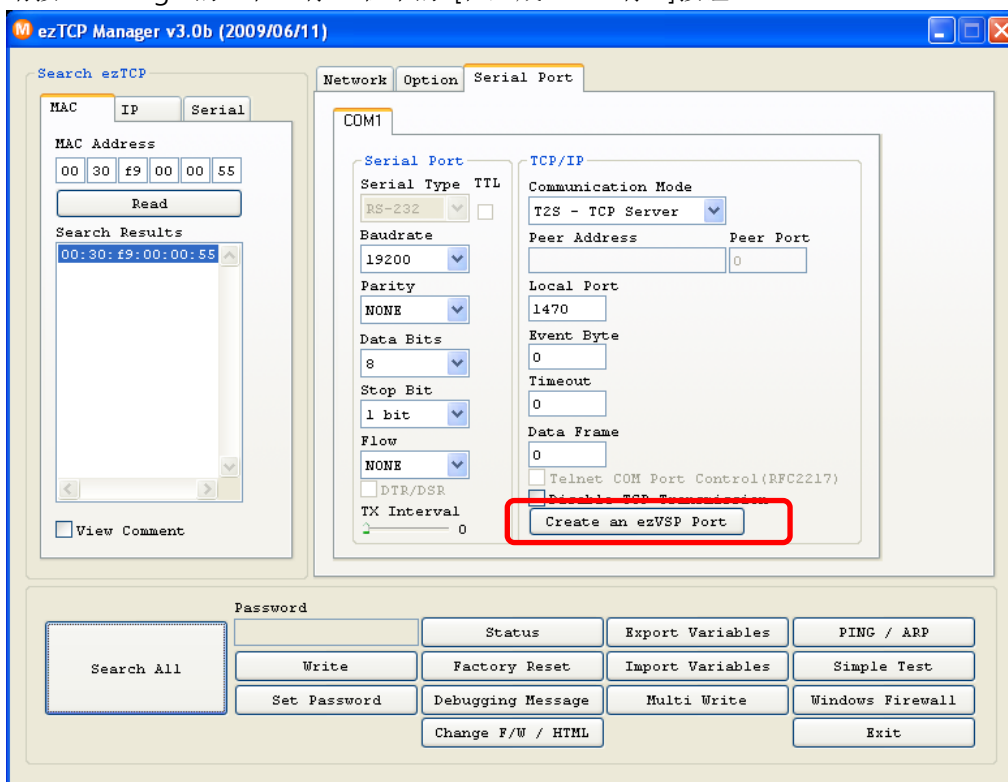


图 3-4 生成虚拟串口端口

如下图生成图片后按确认按钮。

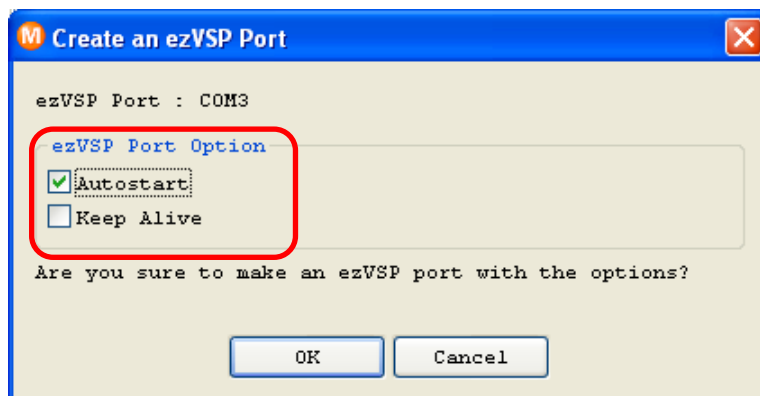


图 3-5 在ezVSP生成端口

完成端口生成后，请在ezVSP开始对应虚拟端口。

*ezVSP是在PC生成虚拟串口端口同 ezTCP 产品的相同角色，详细使用说明及设置，请参考 ezVSP 使用者说明。*

- 确认TCP连接

ezVSP的虚拟端口正常开始运行后，利用SSL的产品（ezTCP）与ezVSP的虚拟端口间的进行了TCP连接。此情况通过ezManager的[STATUS]按钮进行确认。

如下图在“TCP STATE”项目中确认了“COM1 – ESTABLISHED”，在“SSL STATUS”项目中确认了 [State – 7]与 [Cipher – RSA\_AES\_256CBC\_SHA]完成了其通信准备。

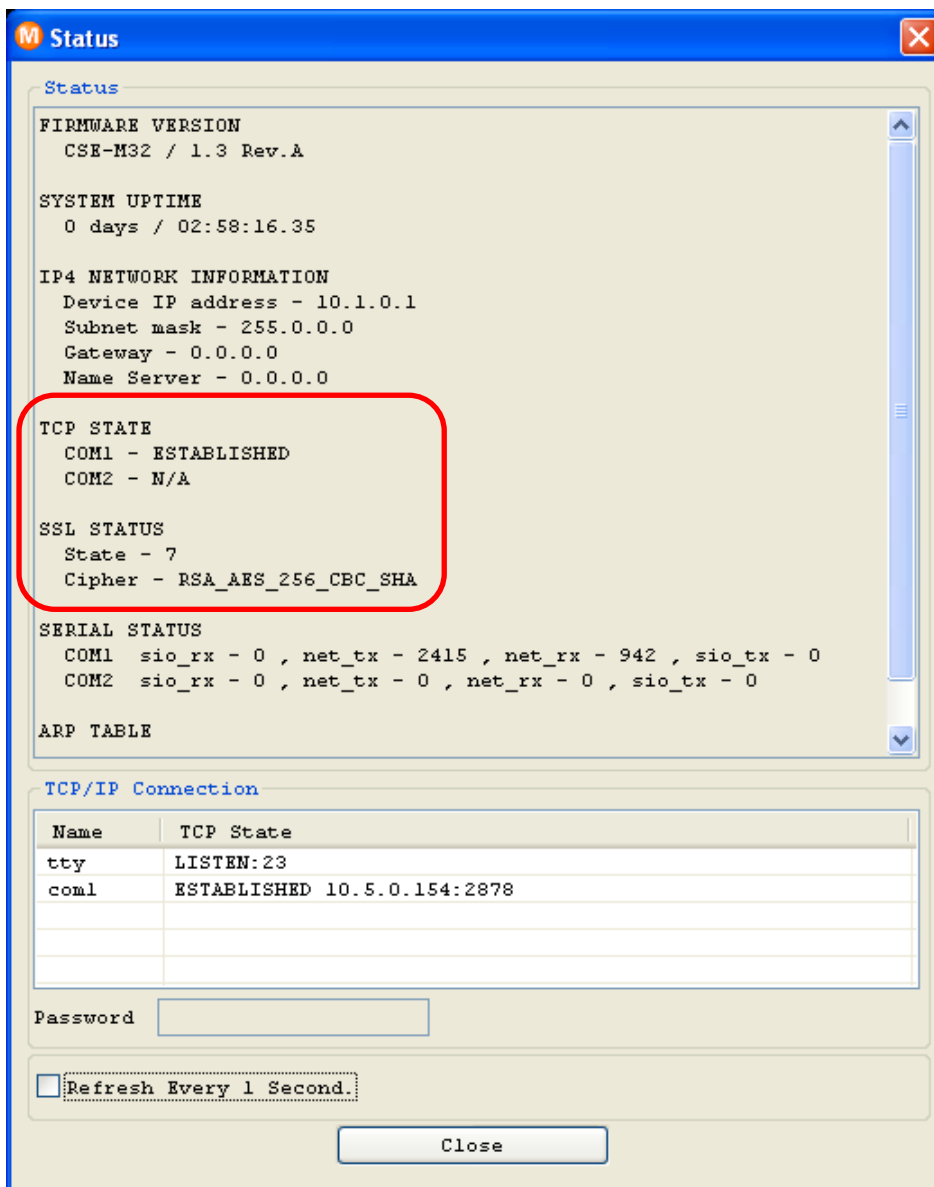


图 3-6 SSL 技能 确认TCP连接

### 3.3 TCP 客户端模式

TCP 客户端模式只能根据 SSL 设定画面使用，ezTCP 要连接的 TCP 服务器也要支援 SSL。同目前确认是否连接到了 TCP 服务器模式，请利用 ezManager 的 [STATUS] 按钮。

## 4 Revision History

Date	Version	Comments
2008.08.28	1.0	Initial Release
2009.06.11	1.1	修正部分用语 增加支援产品 CSE-H25