Application Note

SSL (Secure Socket Layer)

Version 1.1
2009-06-11

SOLLAE SYSTEMS(株) http://www.sollae.co.kr

目录

1 概要 ..... - 2 -

1.1 SSL (Secure Socket Layer) ..... - 2 -
1.2 适用 ..... - 2 -

2 设定 ..... - 3 -

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 生成认证书 ..... - 4 -

3 使用 例 ..... - 9 -

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 -

4 REVISION HISTORY ..... - 15 -

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 生成人证书") 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。

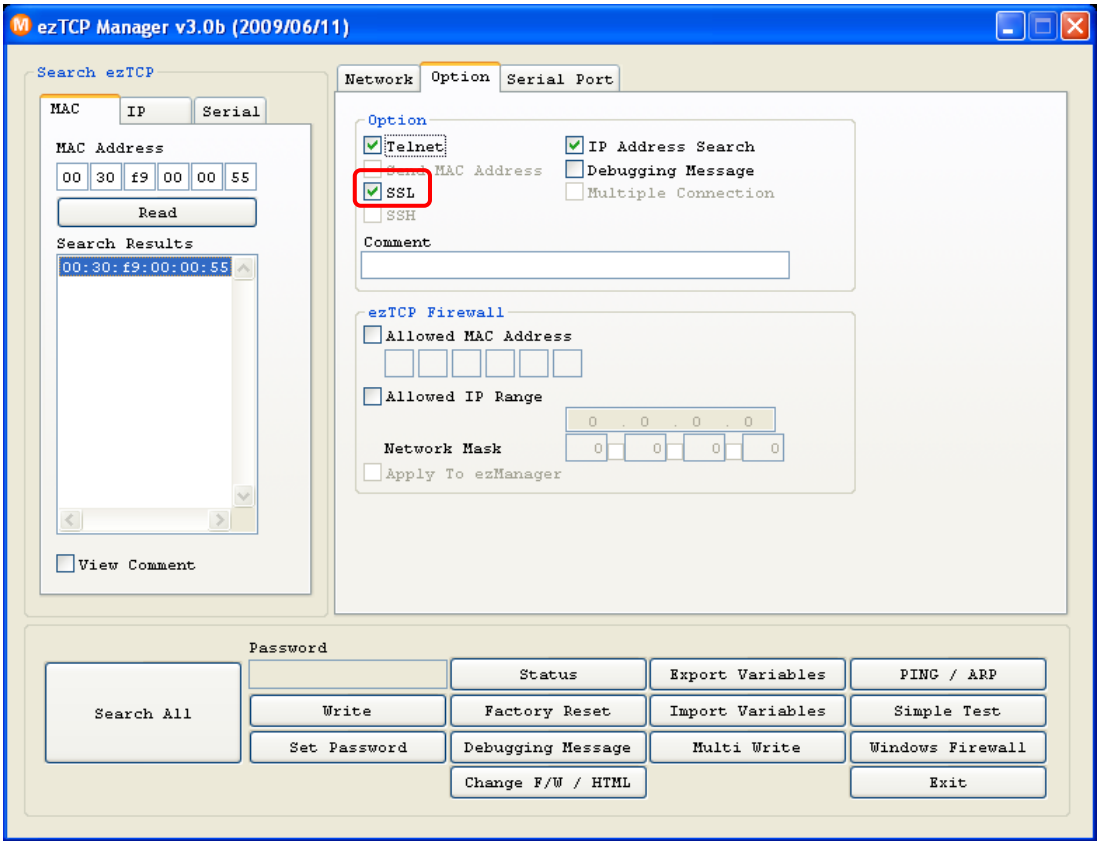

图 2-1 设定"SSL 保安通信" 选项

2.2.3 生成认证书

- 连接到产品（ezTCP）的 Telnet。

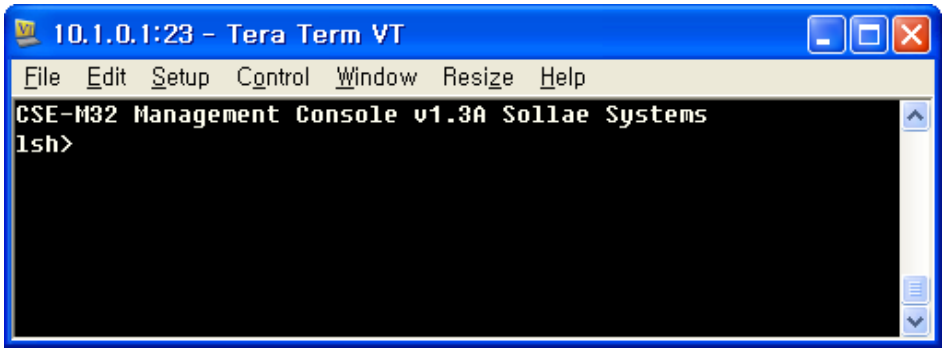

图 2-2 连接 Telnet

- 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。

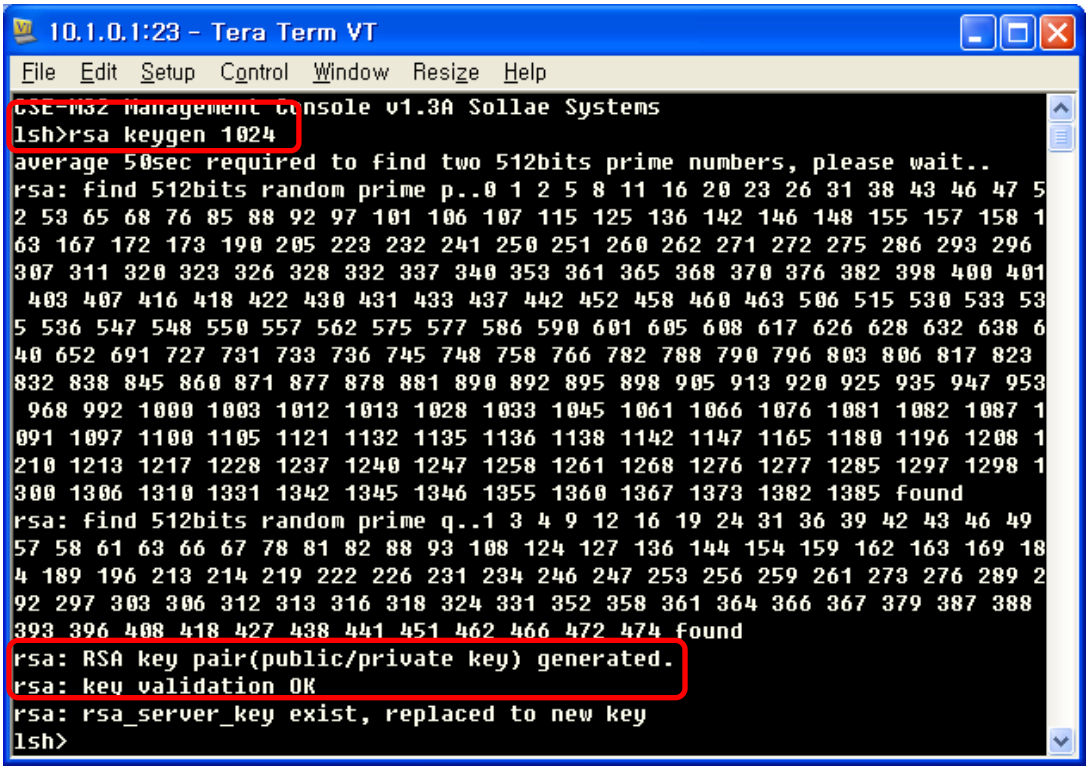

图 2-3 生成RSA KEY

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。

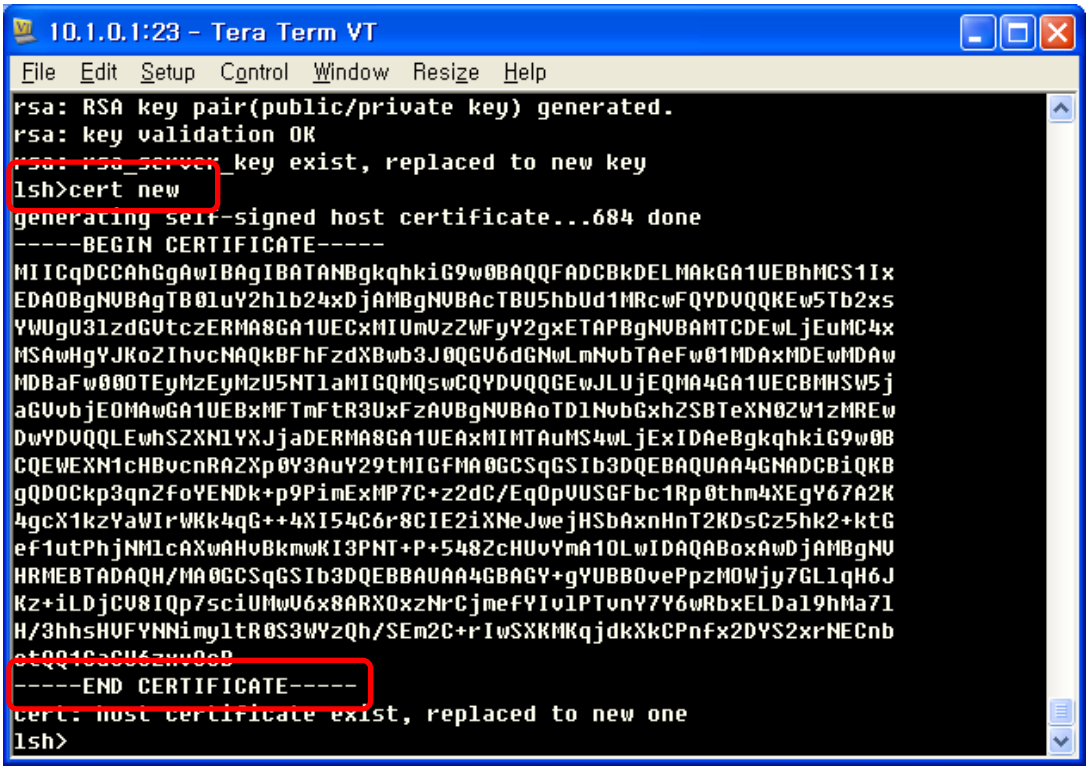

图 2-4 生成认证书

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

☞ ***生成认证书原来的认证书自动更换为新生成的认证书。***

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

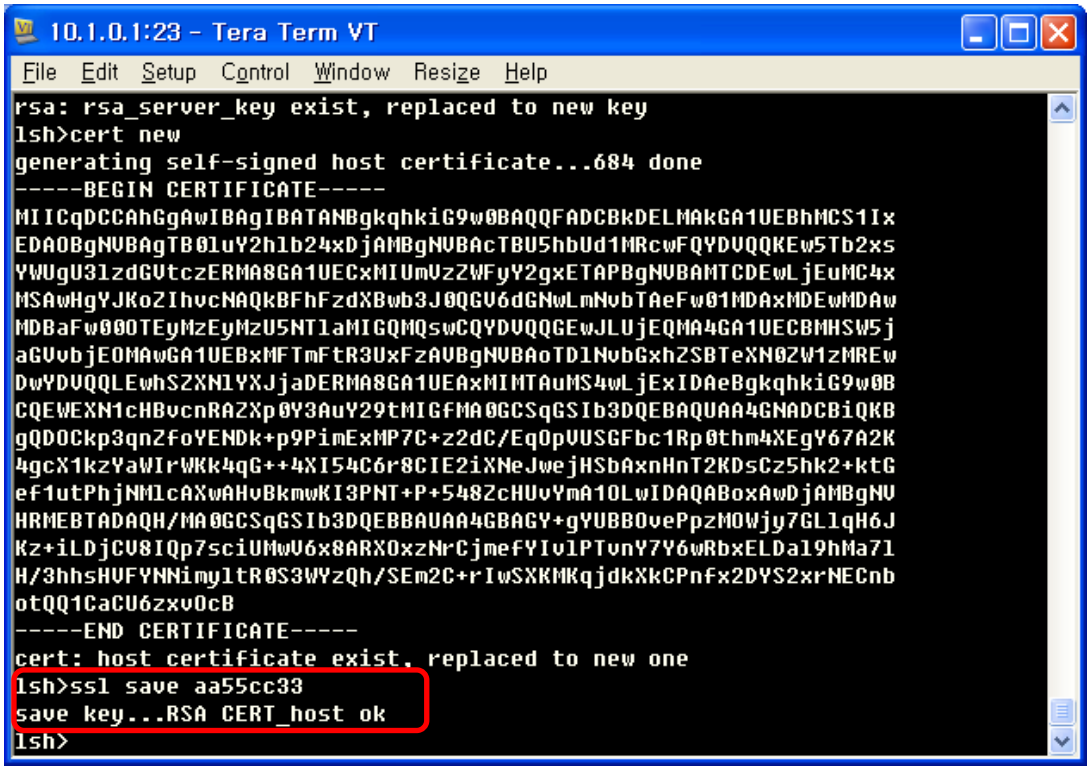
10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Resize Help
rsa: rsa_server_key exist, replaced to new key
lsh>cert new
generating self-signed host certificate...684 done
-----BEGIN CERTIFICATE-----
MIICqDCCAhGgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBkDELMAkGA1UEBhMCS1Ix
EDAOBgNVBAgTB0luY2hlb24xDjAMBgNVBAcTBU5hbUd1MRcwFQYDVQQKEw5Tb2xs
YWUgU3lzdGVtczERMA8GA1UECxMIUmVzZWFyY2gxETAPBgNVBAMTCDEwLjEuMC4x
MSAwHgYJKoZIhvcNAQkBFhFzdXBwb3J0QGV6dGNwLmNvbTAeFw01MDAxMDEwMDAw
MDBaFw00OTEyMzEyMzU5NTlaMIGQMQswCQYDVQQGEwJLUjEQMA4GA1UECBMHSW5j
aGVvbjEOMAwGA1UEBxMFTmFtR3UxFzAVBgNVBAoTDlNvbGxhZSBTeXN0ZW1zMREw
DwYDVQQLEwhSZXNlYXJjaDERMA8GA1UEAxMIMTAuMS4wLjExIDAeBgkqhkiG9w0B
CQEWEXN1cHBvcnRAZXp0Y3AuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDOCkp3qnZfoYENDk+p9PimExMP7C+z2dC/EqOpVUSGFbc1Rp0thm4XEgY67A2K
4gcX1kzYaWIrWKk4qG++4XI54C6r8CIE2iXNeJwejHSbAxnHnT2KDsCz5hk2+ktG
ef1utPhjNM1cAXwAHvBkmwKI3PNT+P+548ZcHUvYmA1OLwIDAQABoxAwDjAMBgNV
HRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAGY+gYUBBOvePpzMOWjy7GL1qH6J
Kz+iLDjCV8IQp7sciUMwV6x8ARXOxzNrCjmefYIv1PTvnY7Y6wRbxELDa19hMa71
H/3hhsHVFYNNimyltR0S3WYzQh/SEm2C+rIwSXKMKqjdkXkCPnfx2DYS2xrNECnb
otQQ1CaCU6zxvOcB
-----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。

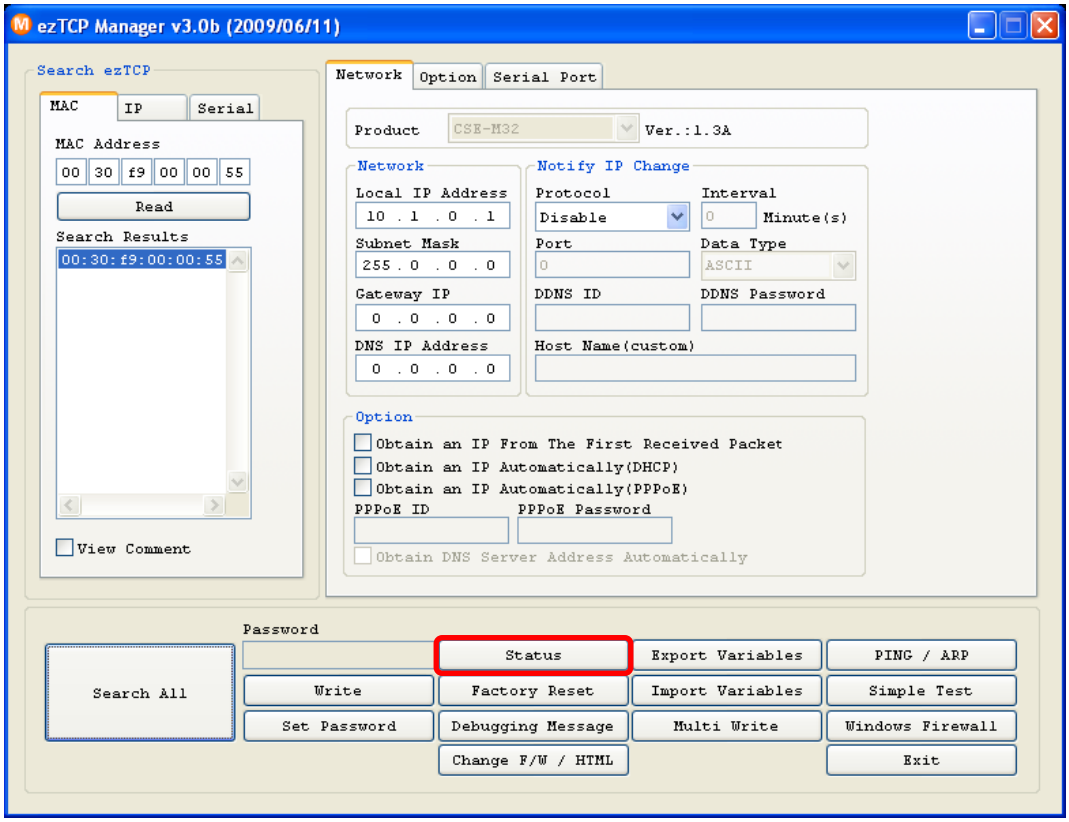

图 3-1 ezManager [STATUS] 按钮

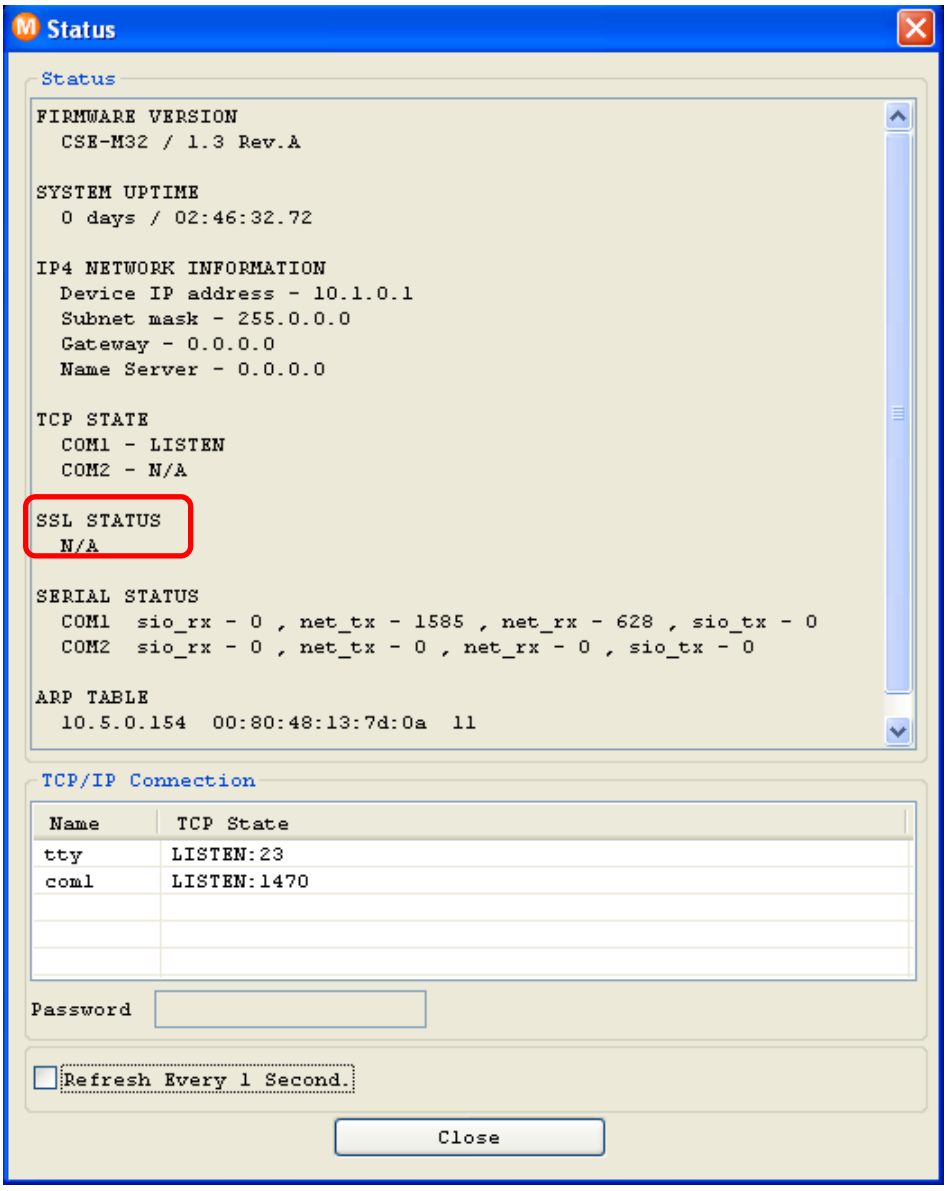

图 3-2 ezManager "STATUS" 画面

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'。此时请确认认证的IP与目前产品中设定的IP是否一致。

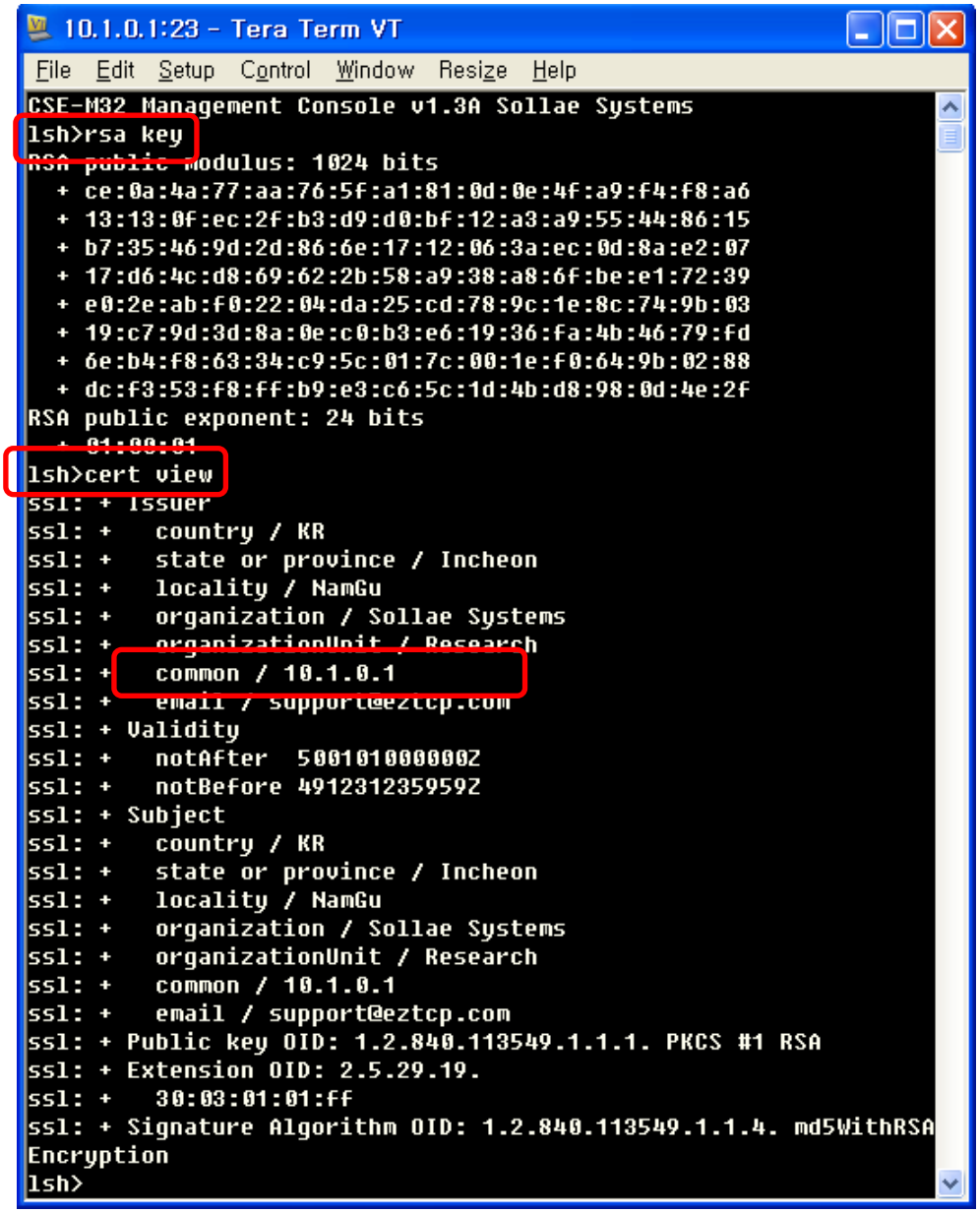

图 3-3 RSA KEY 及确认认证书

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。

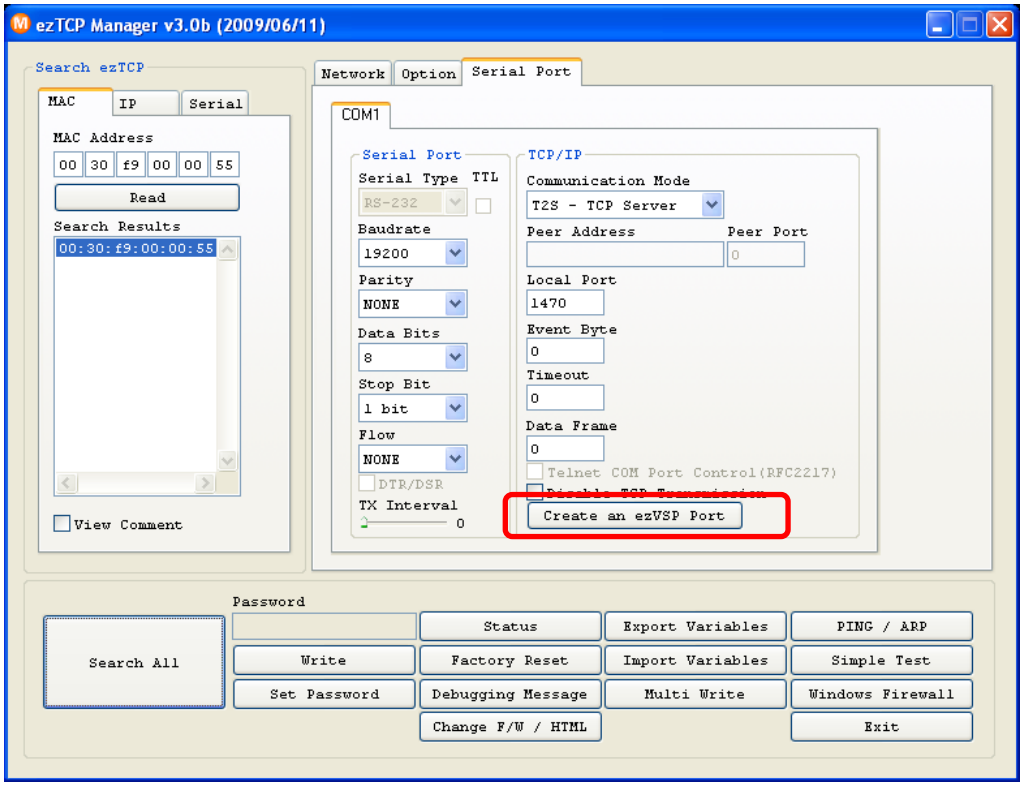

图 3-4 生成虚拟串口端口

如下图生成图片后按确认按钮。

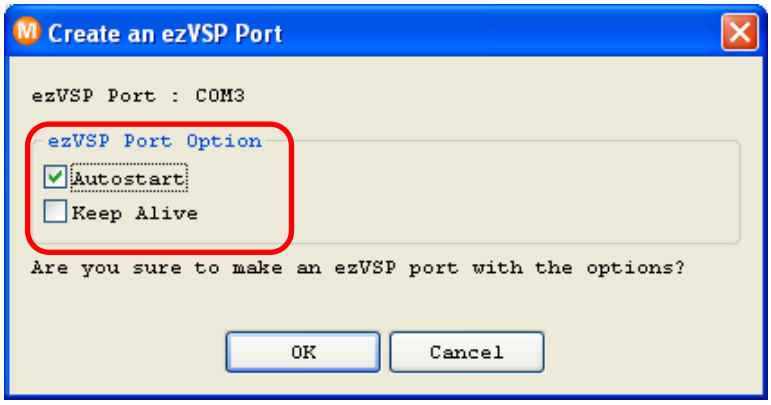

图 3-5 在ezVSP生成端口

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。

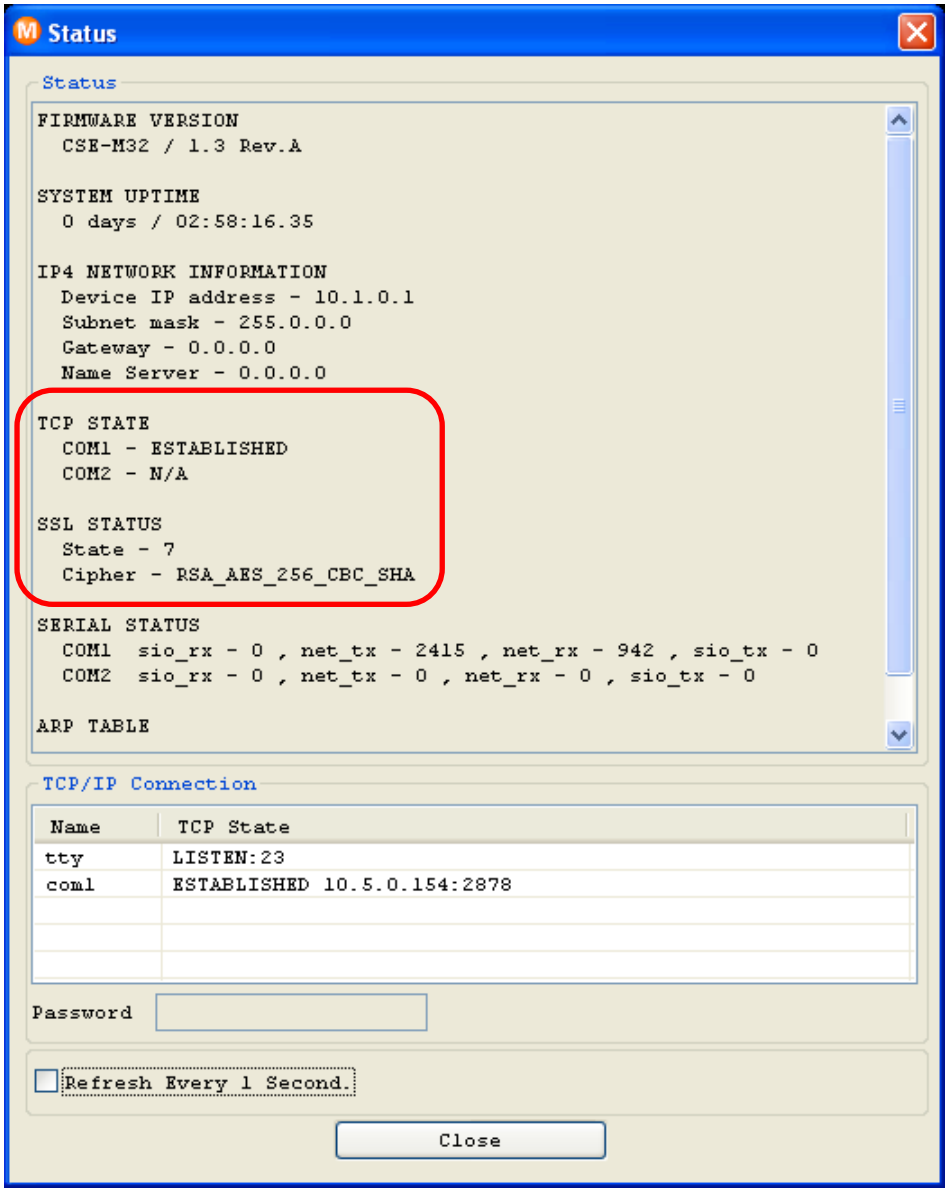

图 3-6 SSL 技能 确认TCP连接

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