Application Note

SSH (Secure Shell) - data

Version 1.0

2008-09-04

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

目录

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

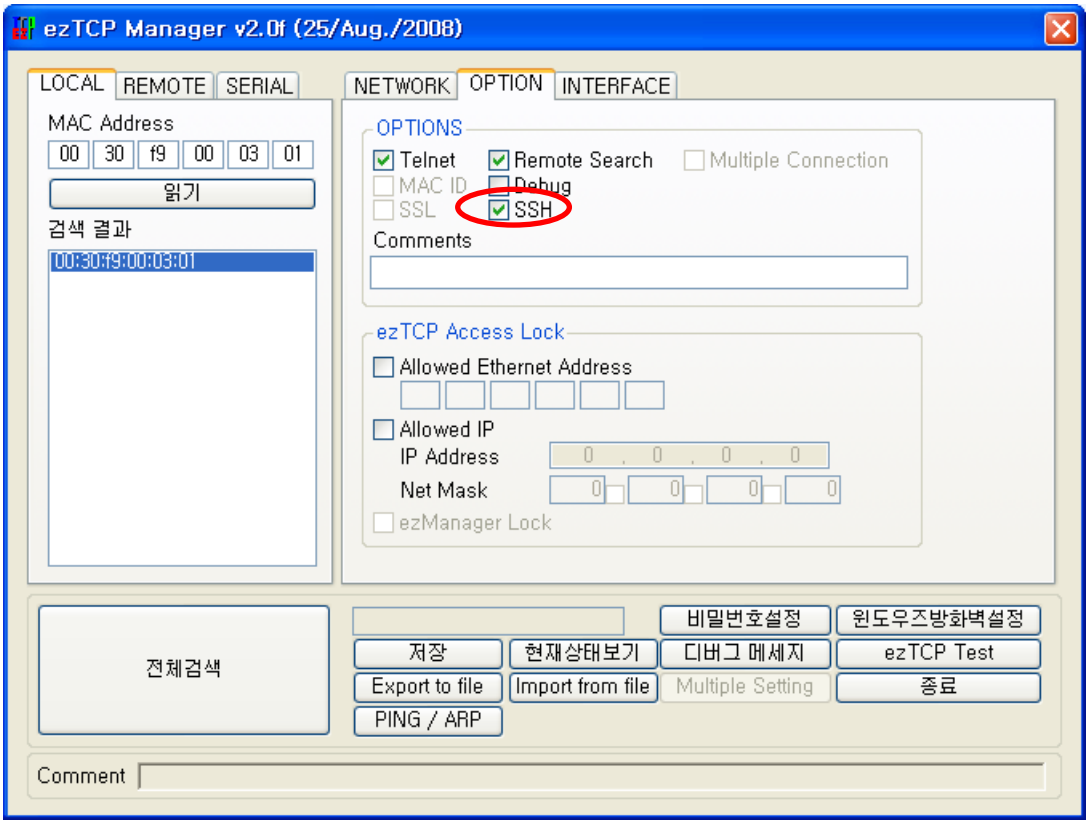
- 只能使用ezTCP Mode T2S(0) – TCP Server 模式。
- 使用SSH技能时，无法使用以下技能。
  SSL, Telnet COM Port Control Option
- 使用SSH技能中各产品限制使用的事项如下。
  CSE-M32, CSE-H20, CSE-H21 –无法使用COM2
  CSE-M73 –无法使用远程控制技能

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。

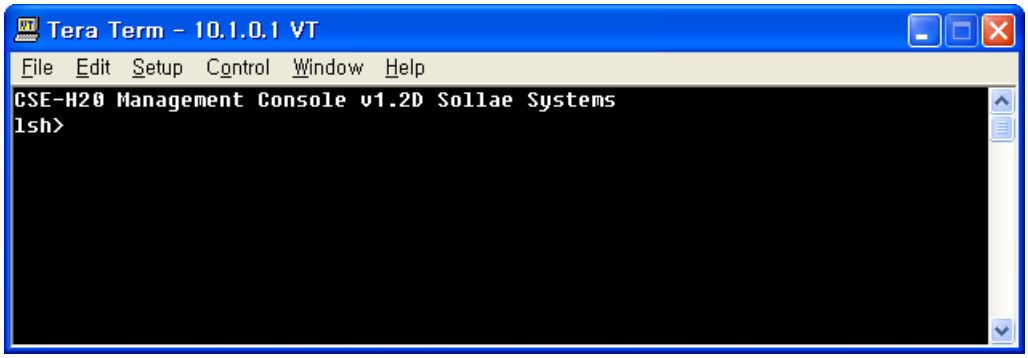


2.2.2 生成 KEY

- 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

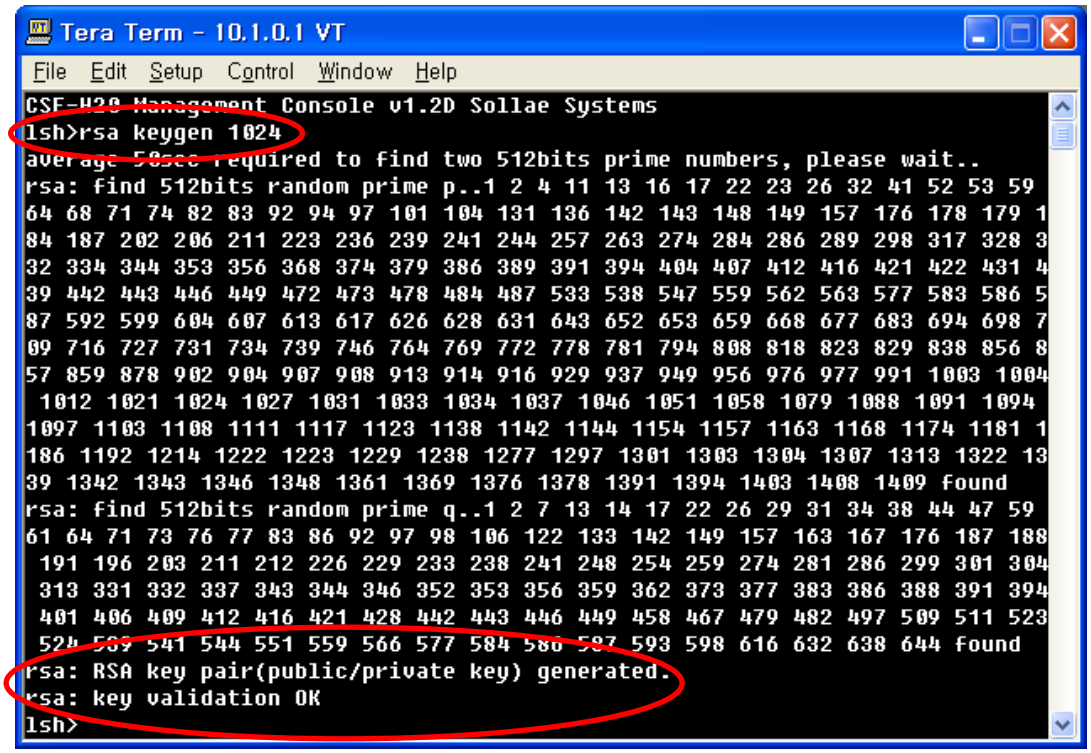
- 连接ezTCP的超级终端。



- 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。

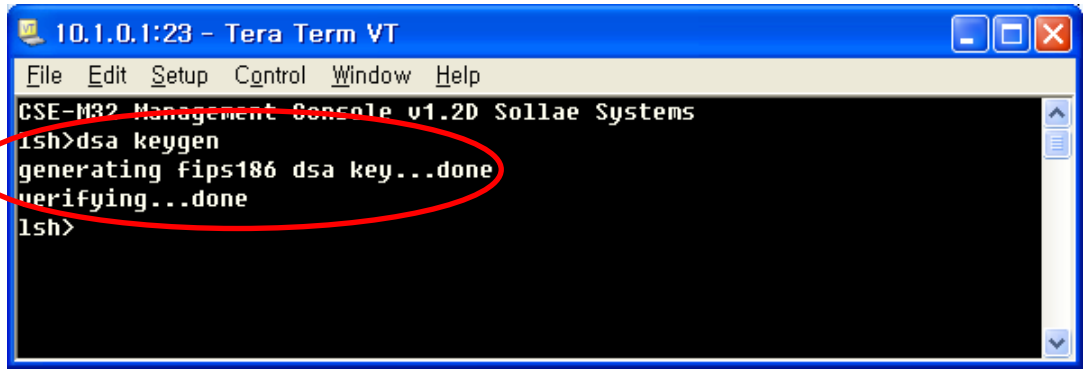


生成的RSA KEY可通过命令 'rsa test'可测试是否按正常形式生成的。

目前产品的RSA KEY可通过'rsa key'命令确认。

- DSA KEY 生成

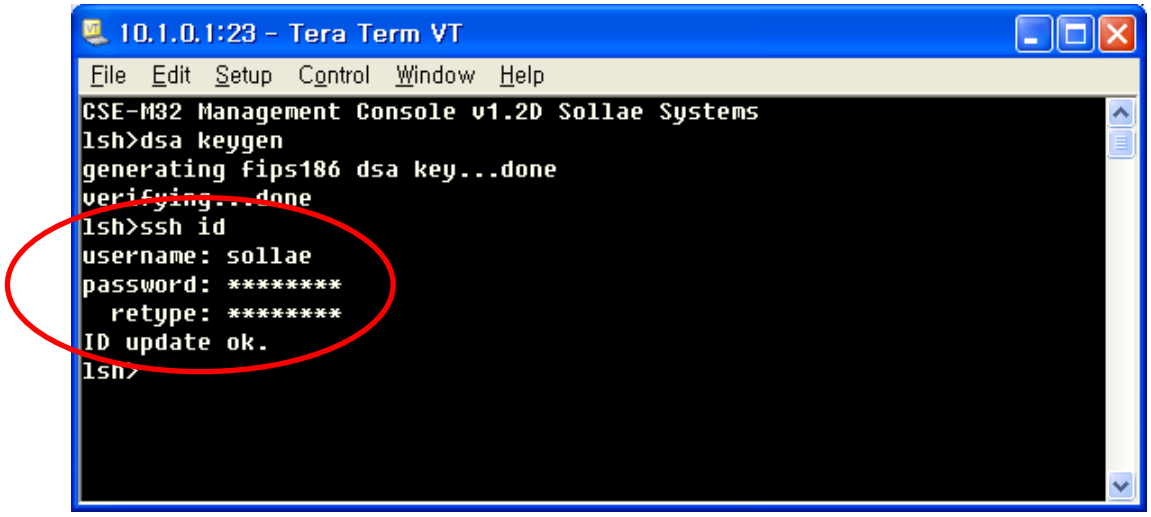
  如RSA KEY正常生成情况下，可通过'dsa keygen' 命令生成DSA KEY。



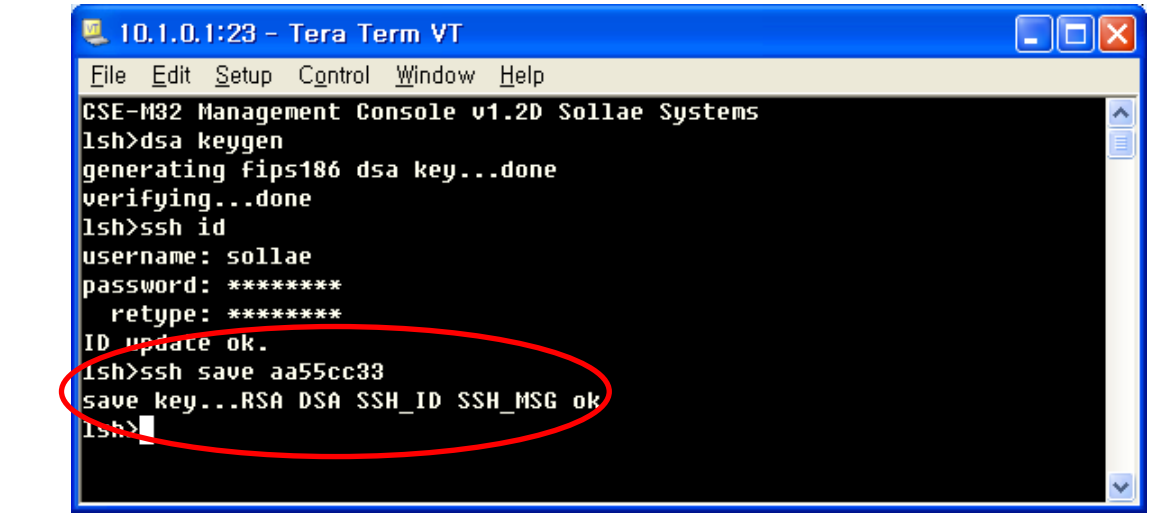
目前生成的DSA KEY는可通过'dsa key' 命令确认。

- 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。



- 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。



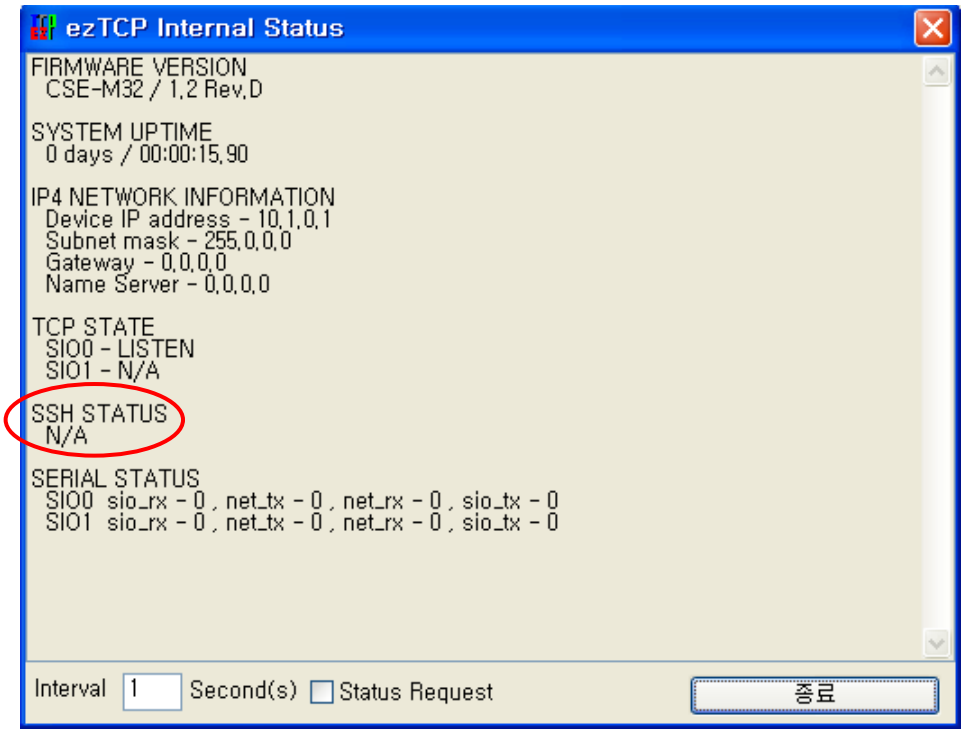
3 使用 例

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

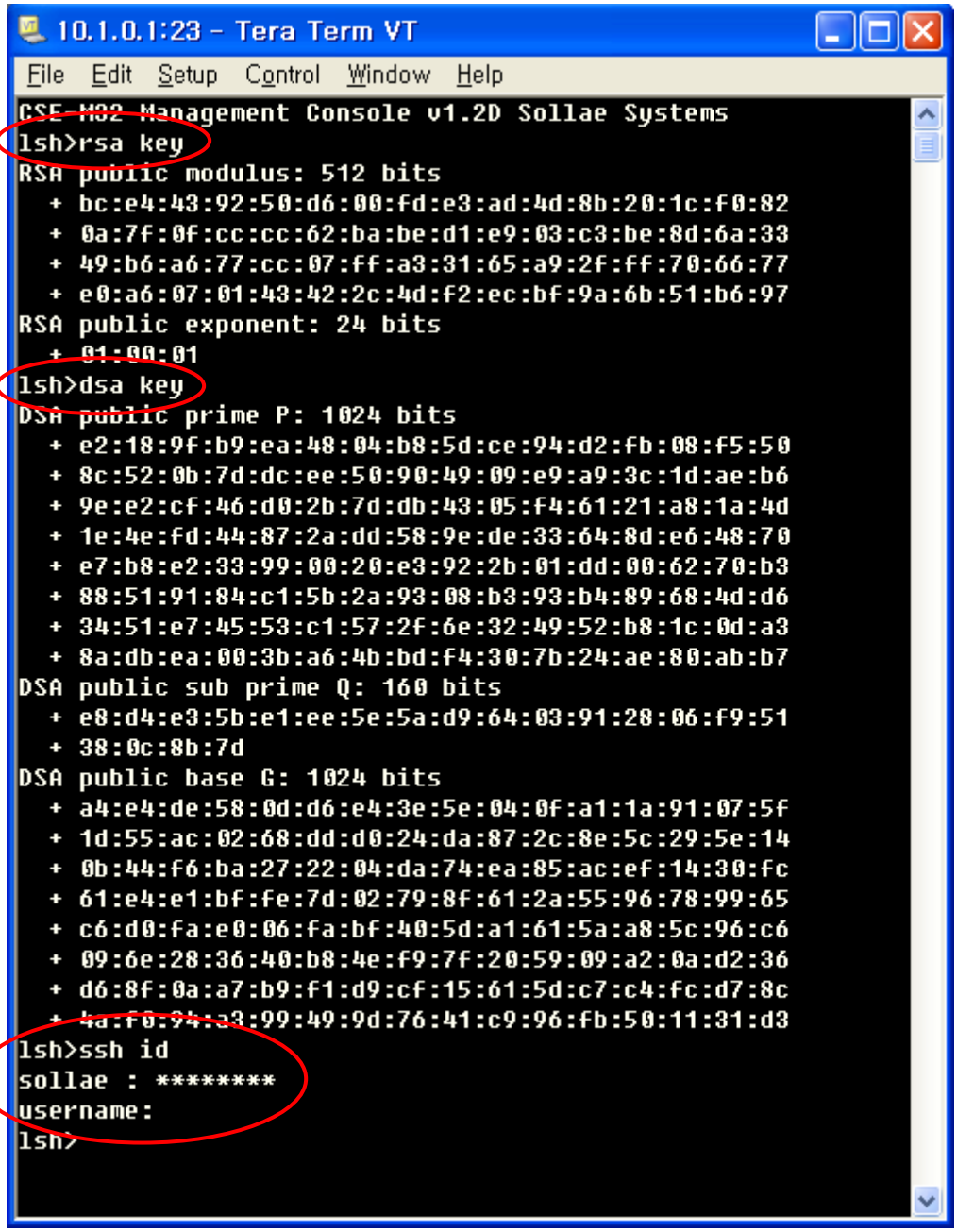
在ezManager按 [STATUS]按钮确认当前状态。



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。



3.1.3 连接

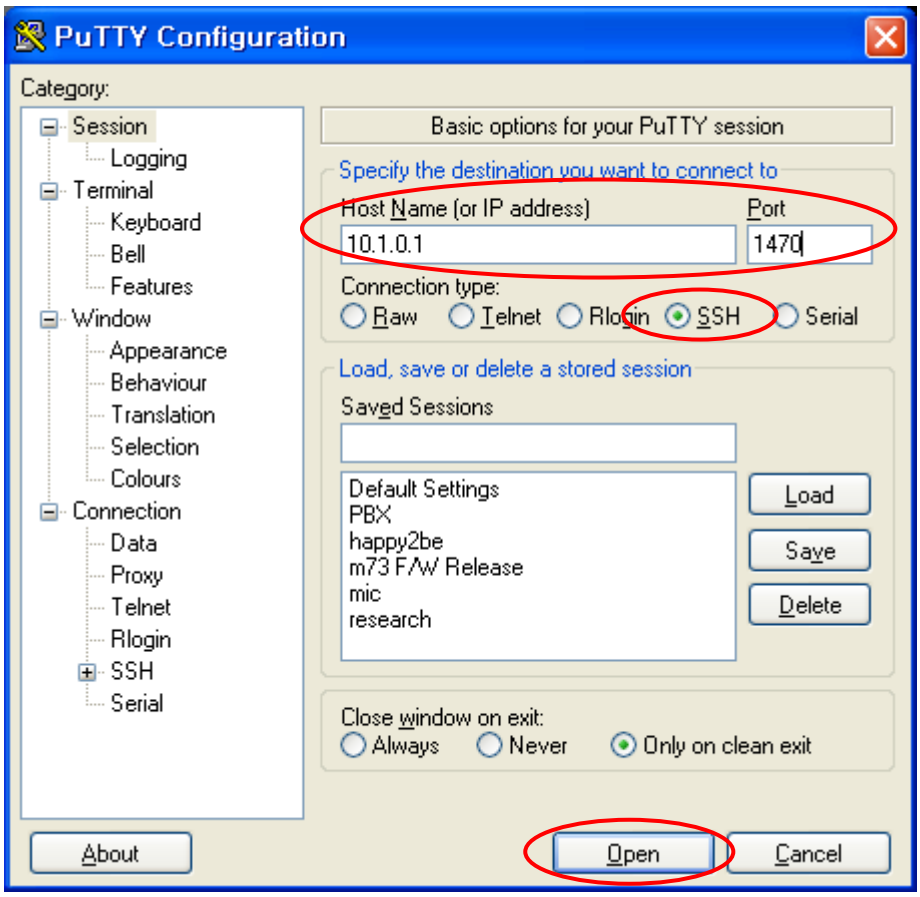
要与已激活SSH技能的ezTCP进行通信，在对方HOST中需要有支持SSH的客户端。此章介绍的是利用商用免费SSH客户端Putty程序测试的过程。

- 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 type이 SSH后按Open按钮。

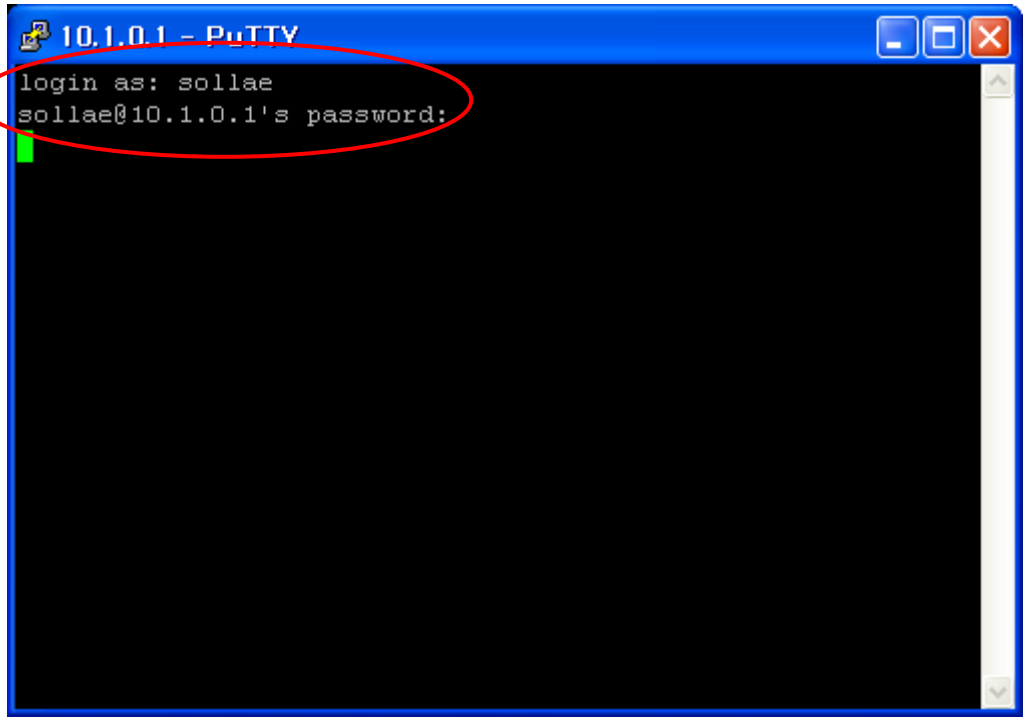
- 确认服务器KEY

  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。

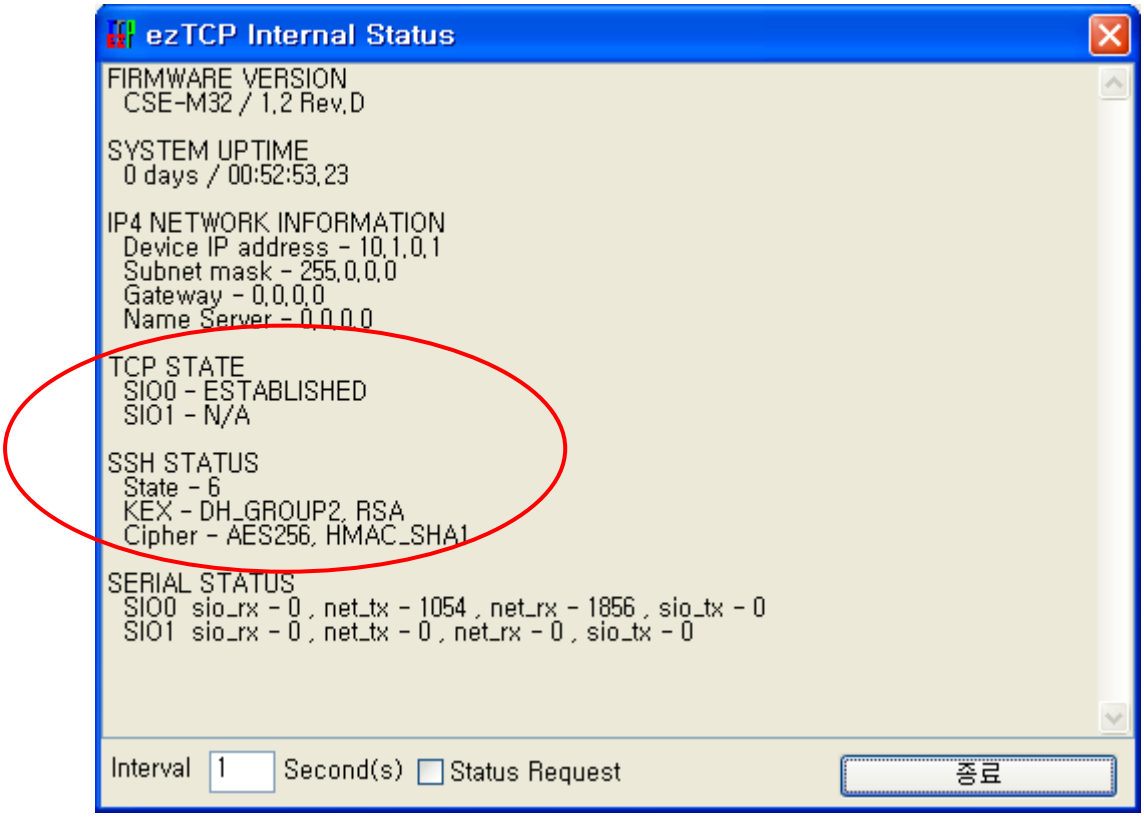
- 登录

  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。

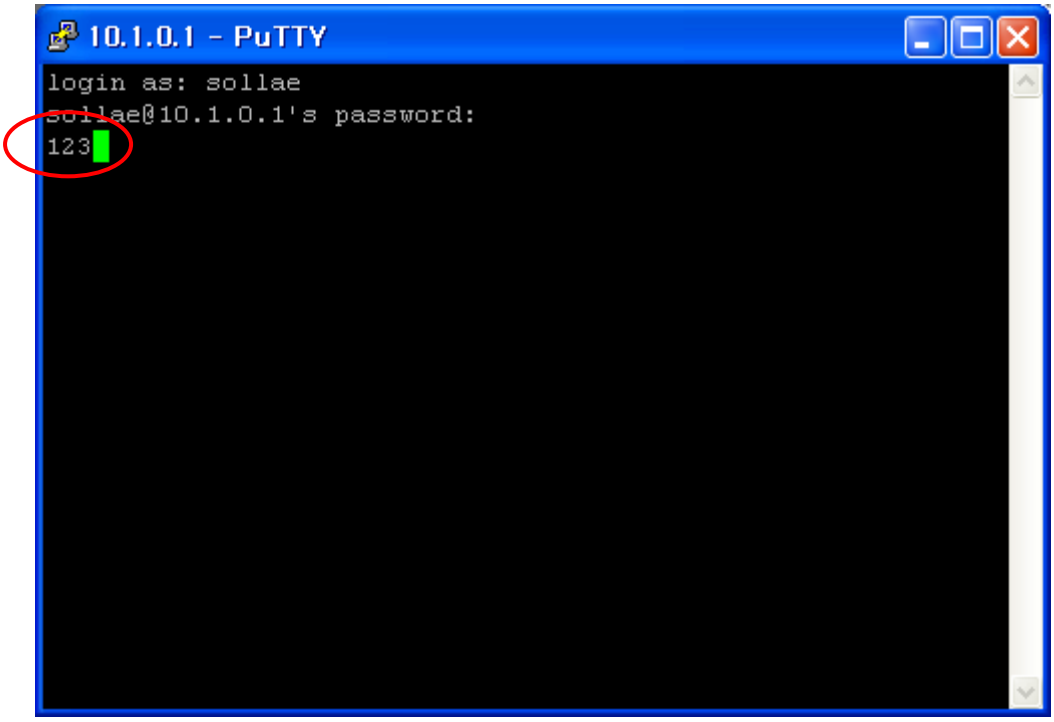


如上图在TCP STATE项目中出现[SIO0 – ESTABLISHED], 出现SSH STATUS 项目的 [State – 6], [Cipher – AES_256, HMAC_SHA1] 可确认为已做好通信准备。

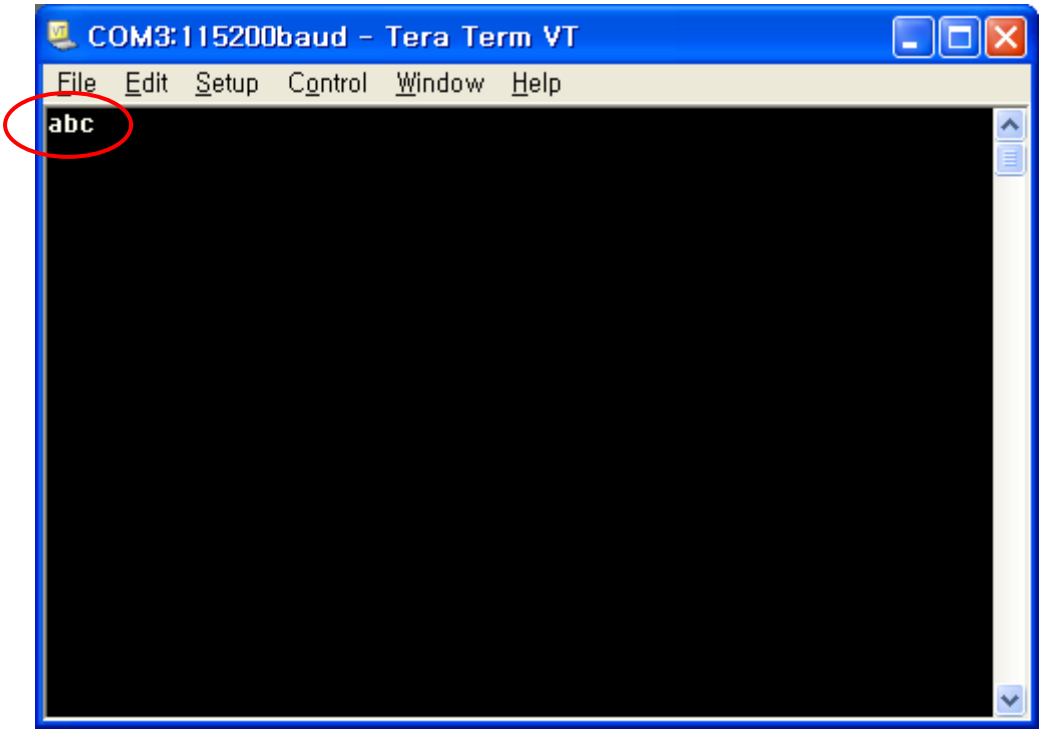
3.2 通信试验

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