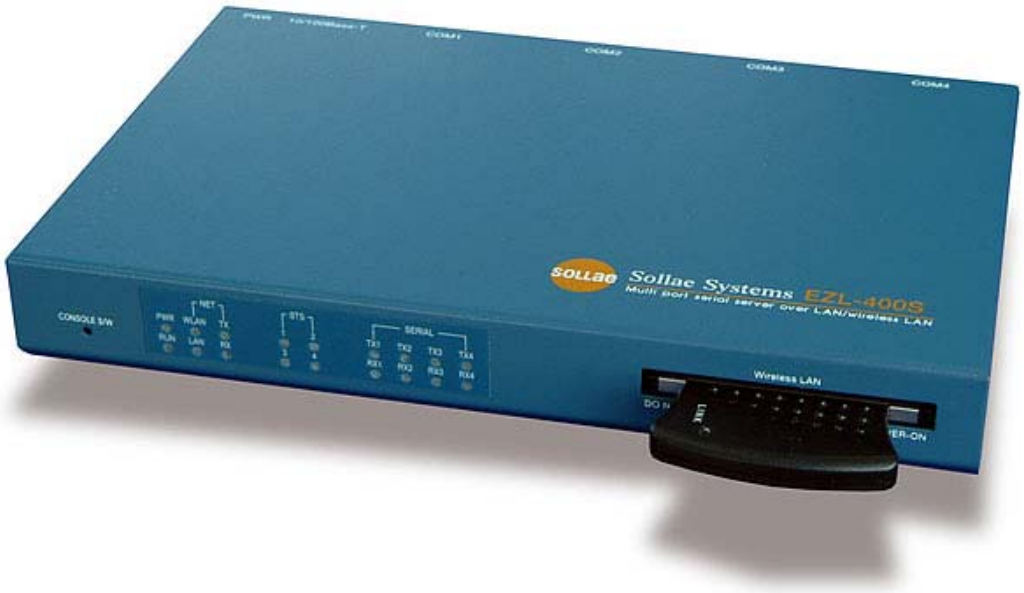
EZL-400S Application Note (002)

SSL(Secure Socket Layer)

Version 1.0



솔내시스템 주식회사

1. 클라이언트 모드에서 SSL 사용하기

클라이언트 모드에서 SSL 기능을 사용하려면 telnet으로 로그인하여 SSL 기능을 활성화시켜 주기만 하면 됩니다.
클라이언트 모드는 COD 모드 또는 ATC 모드에서 atd 명령으로 서버에 접속하는 것을 의미합니다.
SSL을 클라이언트로 사용하려면 통신 대상 서버도 SSL 을 사용해야 합니다.

1.1. SSL 기능 활성화 하기

telnet 클라이언트로 로그인 하여 SSL 기능을 활성화 할 수 있습니다. 다음은 SSL 기능을 활성화 하기 위한 예입니다.

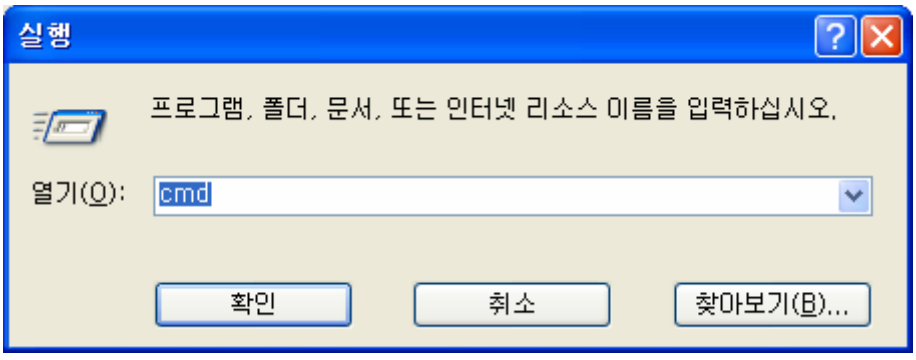
1.1.1. IP 주소 설정

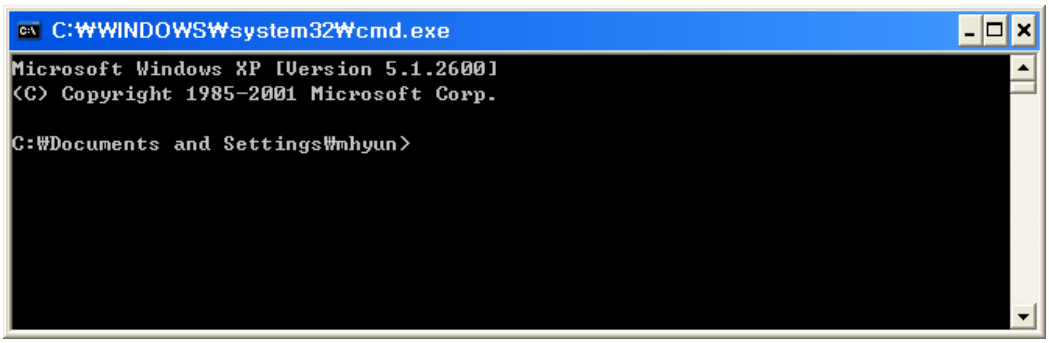
EZL-400S 가 설치된 환경에 맞게 IP 주소관련 항목을 설정해야 합니다. 설정해야 할 IP 주소 항목은 [LOCAL IP ADDRESS], [SUBNET MASK], [GATEWAY IP ADDRESS]입니다.
PC와 EZL-400S의 IP 주소가 다음과 같다는 가정하에 설명하겠습니다.

	PC	EZL-400S
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0
Gateway IP Address	10.1.0.254	10.1.0.254

1.1.2. telnet으로 로그인

윈도우즈 [시작]메뉴에서 [실행] 누르시고 'cmd'를 입력하면 도스창이 나타납니다.

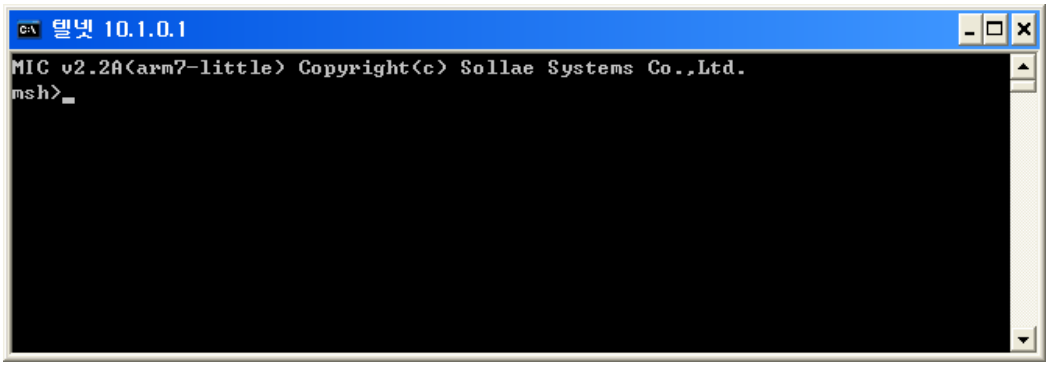




도스창이 나타나면 다음과 같이 입력하여 telnet으로 로그인 합니다.
‘telnet [LOCAL IP ADDRESS]’
[LOCAL IP ADDRESS]는 1.1.1에서 설정한 EZL-400S 의 IP 주소입니다.

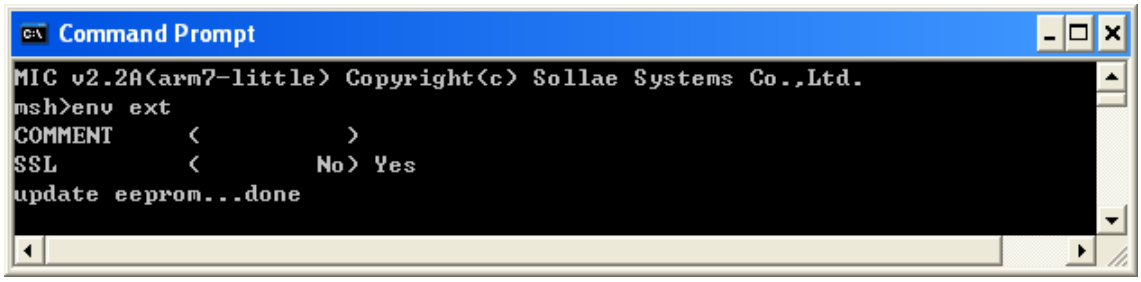
예) telnet 10.1.0.1

아래 그림은 로그인한 그림입니다.



1.1.3. SSL 기능 활성화

‘env ext’ 명령을 입력한 후 SSL 기능 설정 항목인 ‘SSL’에 ‘y’를 입력합니다.



1.1.4. Rebooting

모든 항목들이 지나가면 자동으로 리부팅됩니다.

Console 에서 어떤 명령을 입력할 때 한 항목이라도 변경이 되면 자동으로 리부팅합니다.

1.2. 클라이언트로서 SSL 통신시 주의점

1.2.1. SSL 클라이언트 통신이 가능한 모드

SSL은 TCP 프로토콜 상위에서 동작하는 프로토콜이므로 TCP가 적용되는 통신 모드에서만 통신을 할 수 있습니다.
아래는 SSL 클라이언트 통신을 지원하는 통신모드입니다.

- COD 모드
- ATC 모드에서 'atd' 명령을 사용할 때

2. 서버 모드에서 SSL 사용하기

2.1. SSL 기능 활성화 하기

telnet 클라이언트로 로그인 하여 SSL 기능을 활성화 할 수 있습니다. 다음은 SSL 기능을 활성화 하기 위한 예입니다.

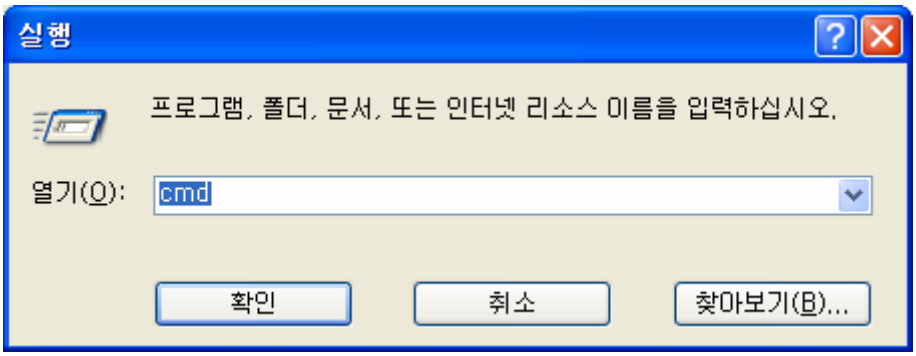
2.1.1. IP 주소 설정

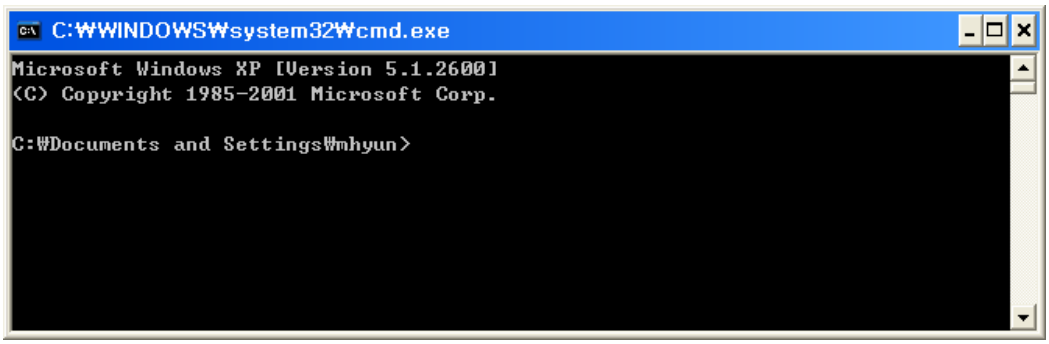
EZL-400S 가 설치된 환경에 맞게 IP 주소관련 항목을 설정해야 합니다. 설정해야 할 IP 주소 항목은 [LOCAL IP ADDRESS], [SUBNET MASK], [GATEWAY IP ADDRESS]입니다.
PC와 EZL-400S의 IP 주소가 다음과 같다는 가정하에 설명하겠습니다.

	PC	EZL-400S
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0
Gateway IP Address	10.1.0.254	10.1.0.254

2.1.2. telnet으로 로그인

윈도우즈 [시작]메뉴에서 [실행] 누르시고 'cmd'를 입력하면 도스창이 나타납니다.

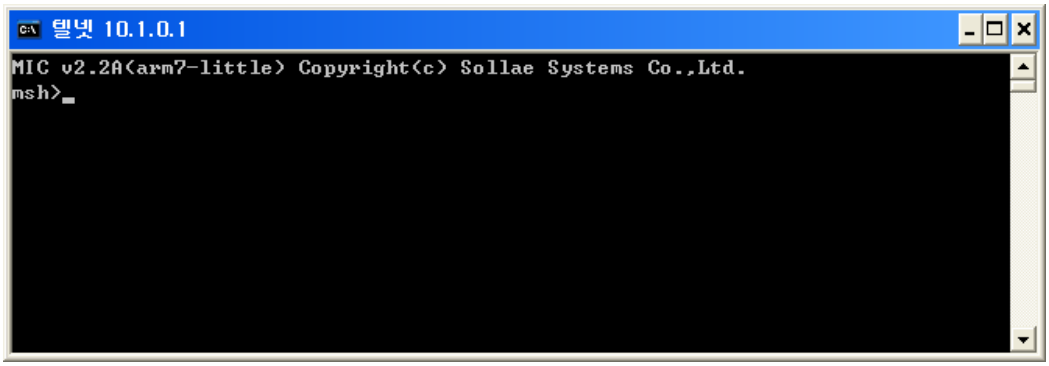




도스창이 나타나면 다음과 같이 입력하여 telnet으로 로그인 합니다.
'telnet [LOCAL IP ADDRESS]'
[LOCAL IP ADDRESS]는 1.1.1에서 설정한 EZL-400S 의 IP 주소입니다.

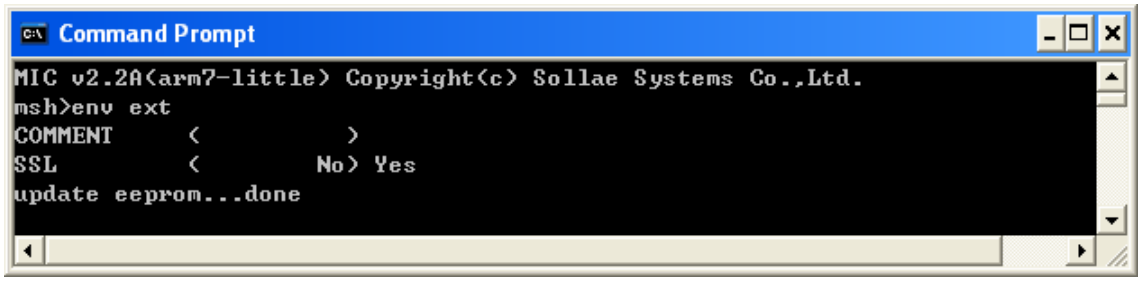
예) telnet 10.1.0.1

아래 그림은 로그인한 그림입니다.



2.1.3. SSL 기능 활성화

'env ext' 명령을 입력한 후 SSL 기능 설정 항목인 'SSL'에 'y'를 입력합니다.



2.1.4. Rebooting

모든 항목들이 지나가면 자동으로 리부팅됩니다.

Console 에서 어떤 명령을 입력할 때 한 항목이라도 변경이 되면 자동으로 리부팅합니다.

2.2. 키 생성

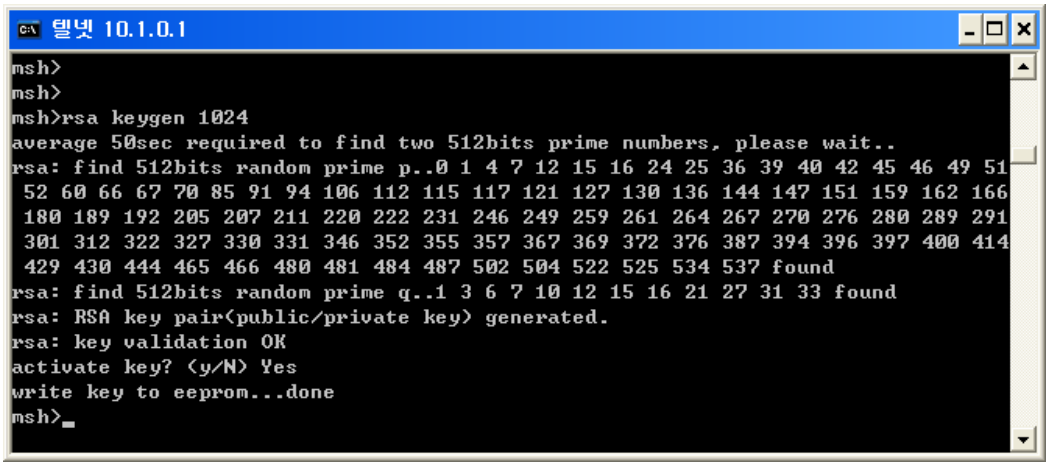
SSL 서버로서 동작하려면 SSL 클라이언트에게 전달할 public key와 SSL 서버 자신이 사용할 private key를 생성해야 합니다.

2.2.1. telnet login

telnet 로그인 상태가 아니라면 2.1 과정으로 telnet 로그인합니다.

2.2.2. 키 생성

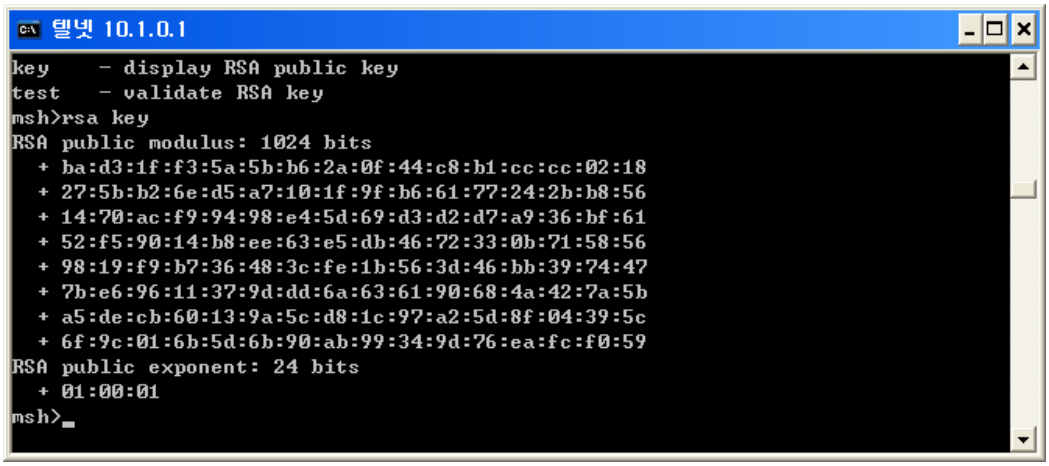
다음의 명령어 형식으로 RSA 키를 생성합니다.
키를 생성할 때 key의 크기에 따라 수분이 걸릴 수도 있습니다.
(명령어형식) rsa keygen [keylength]
[keylength]는 사용하는 키 길이에 따라 512, 768, 1024, 또는 2048를 입력하실 수 있습니다.
키가 길면 길수록 시간이 길어집니다. 예를 들어, 키 길이가 2048 비트인 경우에는 평균적으로 5분정도 소요됩니다.



키를 생성한 후 생성된 키를 비휘발성 메모리에 저장여부를 질의합니다. 이때 'y'를 눌러 생성된 키를 비휘발성 메모리에 저장합니다.

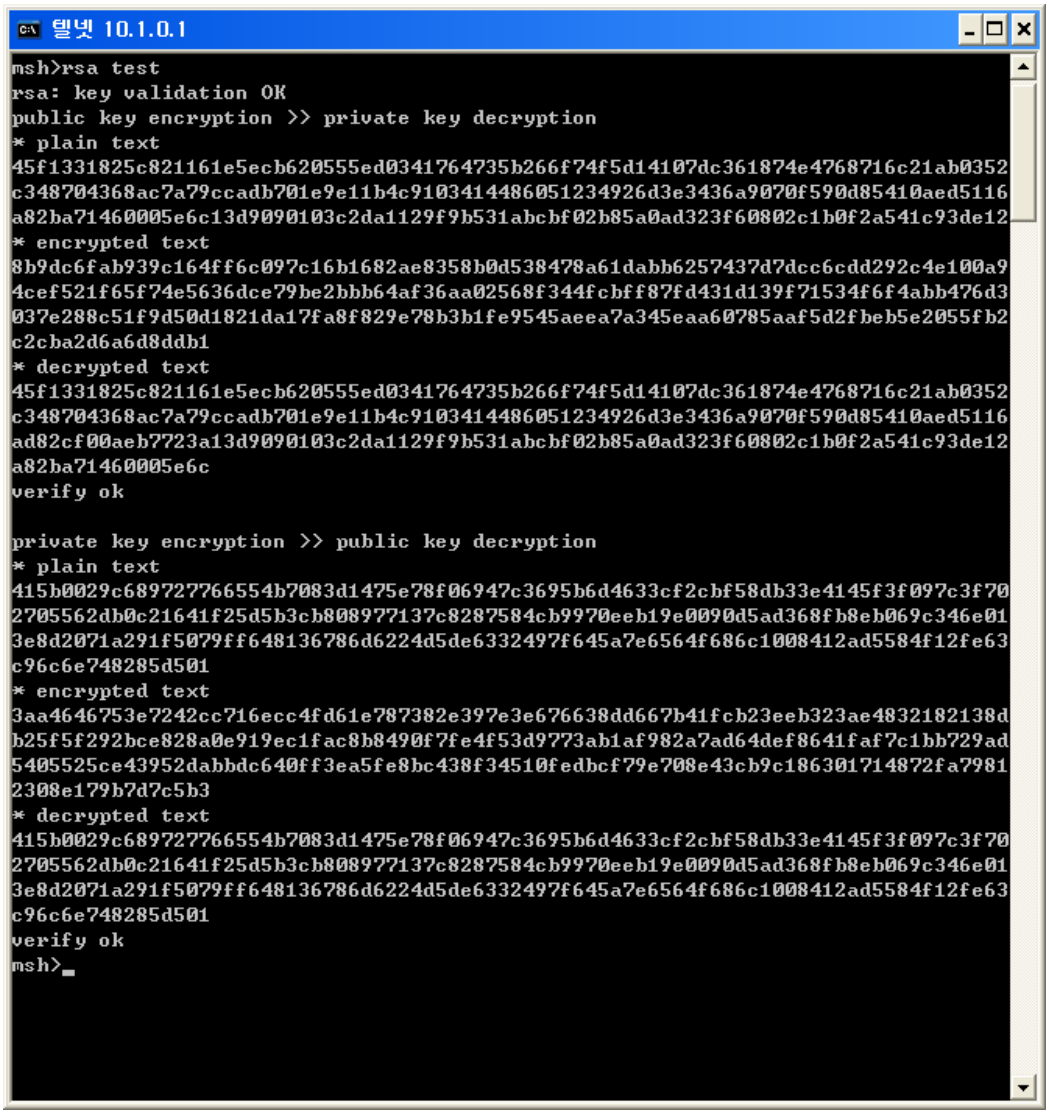
2.2.3. RSA public key 확인

‘rsa key’ 명령으로 RSA public key를 확인할 수 있습니다.



2.2.4. RSA 키 테스트

생성된 RSA private key와 public key를 테스트합니다. 테스트는 public key로 암호화한 임의의 텍스트를 private key로 암호를 푼 다음 원래의 텍스트와 같은지 확인하고, private key로 암호화한 임의의 텍스트를 public key로 암호를 푼 다음음 원래의 텍스트와 같은지 확인합니다.

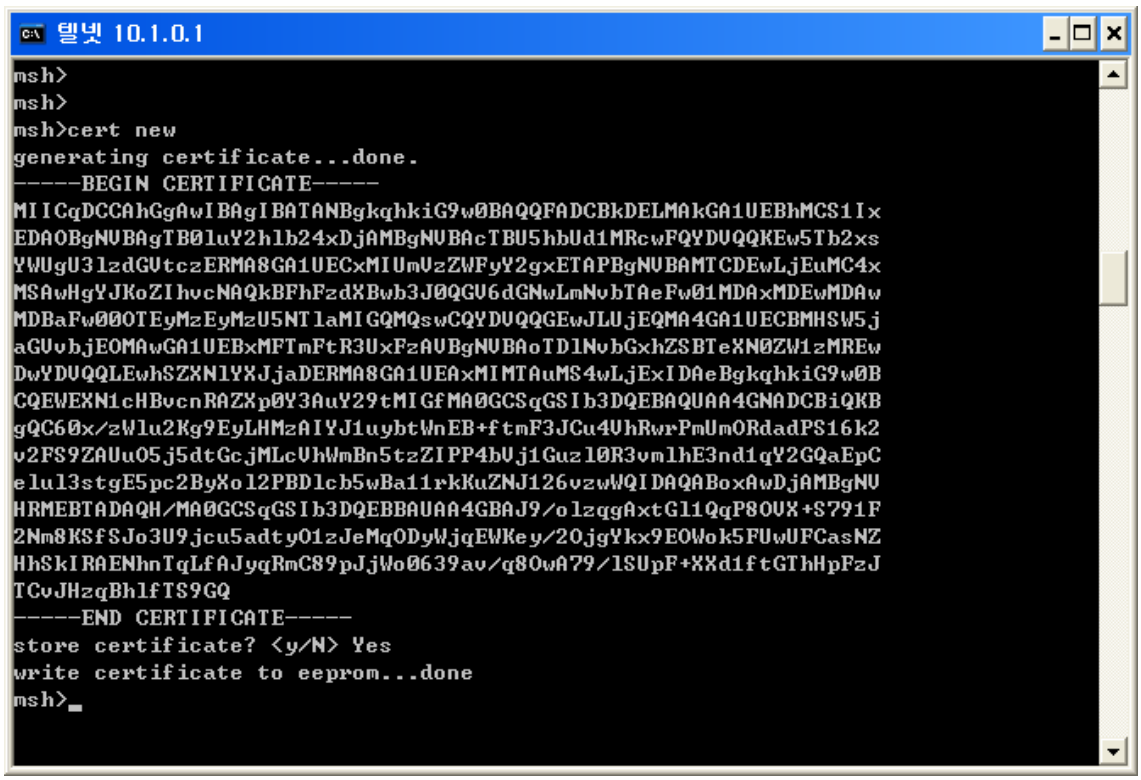


2.3. 인증서 생성

SSL 서버는 인증서를 가지고 있어야 합니다. 공인 인증서를 받지 않고 자체적인 인증서를 생성해서 사용할 수 있습니다.

2.3.1. 인증서 생성

‘cert new’ 명령으로 인증서를 생성할 수 있습니다. ‘cert new’ 명령에 EZL-400S 는 인증서를 생성하고, 인증서에 자체적으로 싸인을 합니다. 인증서 생성이 끝나면 비휘발성 메모리에 저장 여부를 묻습니다. ‘y’라고 입력하면 자체 생성된 인증서가 비휘발성 메모리에 저장됩니다.



인증서에 자신의 IP의 정보도 있으므로 IP 주소가 바뀌면 인증서를 새로 생성해야 합니다.