작성자: 방보현

작성일: 2016-03-07

제목: openssl server 사용방법.

내용

1. Self-signed certificate 생성
   1. 개인키 생성

/> openssl genrsa –des3 –out server.key 2048

(상업적으로 사용될 때 이 키는 절대 유출되지 않도록 주의해야 한다.)

* 1. 인증 요청서 생성

/> openssl req –new –key server.key –out server.csr

(이 때 형식에 맞도록 인증 요청서 내용을 작성한다.)

* 1. 인증서 생성

/> openssl x509 req –days 3650 –in server.csr –signkey server.key –out server.crt

(“server.crt”가 최종적으로 생성된 인증서이다.)

1. 인증서 복사 및 서버 구동
   1. 인증서를 메모장으로 연 후 내용을 펌웨어에 포함시켜야 한다.
      1. certificate.h에 인증서를 복사 후 c언어 형식으로 변경한다.
   2. 서버 구동

/> openssl s\_server –accept 443 –cert server.crt –key server.key

1. 테스트
   1. 서버가 구동된 후 클라이언트 접속이 완료되면 키보드 입력을 통해 원하는 내용을 클라이언트에게 전송할 수 있으며 클라이언트에서 전송된 내용도 표시된다.