X509 인증서

OPENSSL

- Openssl
  - 방대한 암호, 인증서 관련도구
  - 간단하게 X.509 인증서 생성 가능
  - CLI, lib
- Openssl 설치

  $ sudo apt install openssl

- Openssl CLI 실행

  $ openssl

  OpenSSL > help

  OpenSSL > 명령어 –help

- Console command 도 가능

  $ openssl 명령어 파라메터

CA 인증서 만들기

CA 인증서 만들기

- CA의 Self signed 인증서를 만든다
- CA key 생성

  $ openssl genrsa –out myCA.key 2048

- 인증서 발급 (self sign)
  - CN : 이니셜CA ex) dschoiCA

  $ openssl req –x509 –new –nodes –key myCA.key –days 3650 –out myCA.pem

인증서 만들기

- 인증서 발급 요청 만들기
  - 키 생성

    $ openssl genrsa –out myPri.key 2048

  - 인증요청서 (CSR) 만들기 : C -> CA
    - PKCS#10
    - Public key
    - proof of possession 서명 : 공개키에 대한 비밀키 소유 증명
    - Subject name : CN

    $ openssl req –new –key myPri.key –out myCert.csr

- 인증서 발급
  - myCA 키로 서명

    $ openssl x509 –req –in myCert.csr –CA myCA.pem –CAkey myCA.key –CAcreateserial –out myCert.crt –days 365

인증서 검증

- 특정 SSL 서버 인증서 체인 검증
  - CAfile 은 /etc/ssl/certs 폴더에 있음 (trust anchor)

    $ openssl s_client –connect www.google.com:443

- 내가 만든 인증서 체인 검증하기
  - root CA 지정

    $ openssl verify –show_chain –CAfile myCA.pem myCert.crt

  - 중간 CA 포함시

    –untrusted 중간CA파일

  - 등록된 root CA는 지정 필요 없음

ROOT CA 인증서 INSTALL

- CA cert install
  - PEM type을 DER type으로 변경

    $ openssl x509 –in myCA.pem –inform PEM –out myCA.crt

  - 인증서 import 폴더 생성 및 copy

    $ sudo mkdir /usr/local/share/ca-certificates

    $ sudo cp myCA.crt /usr/local/share/ca-certificates

  - install

    $ sudo update-ca-certificates

  - 설치 위치

    /etc/ssl/certs/ca-certificates.crt

과제1

- rootCA , 중간 CA, 사용자 인증서 만들기 (1점)
  - CN=이니셜ROOT, 이니셜CA, 이니셜
  - 파일명도 상기.확장자
  - 인증서 파일 3개 제출 (pri key 파일 제외)

- rootCA 인증서만 install (1점)
  - install 결과화면 캡처 1-1.jpg

- 인증서 체인 verify (1점)
  - -CAfile 옵션 빼고, -untrusted 옵션만 사용
  - verify 명령 및 결과 화면 캡처 1-2.jpg