인증서 포맷 정리

.pem

```
Privacy Enhanced Mail
Base64 인코딩 된 ACSII 텍스트 (notepad에서 열어볼 수 있음)
산업 표준 포맷
루트인증서, 체인인증서, SSL 발급 요청 시 사용되는 포맷
```

.crt

```
거의 대부분(99%) PEM 포맷
유닉스/리눅스 기반
```

.cer

```
거의 대부분(99%) PEM 포맷
윈도우 기반
```

.csr

```
거의 대부분(99%) PEM 포맷
SSL 발급 신청을 위해 파일 내용을 CA에 제출할 때 사용
PKCS#10
```

.der

```
Distinguished Encoding Representation (DER)
바이너리 포맷 (notepad 등으로 열어볼 수 없음)
```

.pfx/.p12

```
PKCS#12 바이너리 포맷
개인키, 서버인증서, 루트인증서, 체인인증서를 담을 수 있음
바이너리 이진 파일
PKCS#12 -> 인증서 + 개인키 .... 인증서 내보내기
```

.p7b/.p7c

```
PKCS#7 포맷  ..... 전자봉투
서버인증서, 루트인증서, 체인인증서 모두 담을 수 있음 (개인키는 포함하지 않음)
b64 텍스트 파일

※ 참고 ※
[안드로이드]
JAR로 서명한 v1체계 서명의 경우 META-INF/ 에 나열된 .RSA|DSA|EC 서명은 Signed
Data 구조가 있는 PKCS#7 CMS 입니다.
```

.key

```
주로 openssl 및 자바에서 개인키 파일임을 구분하기 위해서 사용하는 확장자
PEM 포맷일 수 있고, DER 포맷일 수도 있음
```

.jks

```
Java Key Store
Java 기반 독자 인증서
바이너리 포맷
pfx와 마찬가지로 개인키, 서버인증서, 루트인증서, 체인인증서를 모두 담을 수 있음
Java기반의 Tomcat 서버에서 SSL 적용시 가장 많이 사용
```

출처

- PEM 과 CER/DER/CRT/CSR 형식 파일이란?
- SSL 인증서 파일 포맷 종류 - crt, cer, csr, pem, der, pfx, p12, p7b, jks, key
- 안드로이드 .RSA 파일 관련