3강 인증서, 프로비저닝, 코드서명

- iOS 앱 서명 개요

  실제로 우리는 다양한 계약, 사안에 대한 서명을 합니다. 우리는 왜 계약에 서명합니까? 서명은 우리에게 무엇을 의미하며 왜 중요할까요? 계약서에 서명하면 합법적으로 우리를 보호할 수 있기 때문입니다.

  계약 조항 및 조건을 변경할 수 없고, 신뢰할 수 있는 기관에서 증빙하는 계약이 체결되는 동안 서명은 보안을 보장합니다. (보안, 안전, 신뢰가 제공)

  마찬가지로 iOS 코드 서명은 모든 형태의 코드, 리소스, 설정파일 등에 디지털 서명을 하는 과정입니다. 누가 코드를 작성했는지 확인하고 코드가 변경되지 않았음을 보장하기 위함입니다.

  코드 서명은 암호화 해시를 사용하여 진위를 확인하며 소프트웨어 코드의 무결성 및 신원을 보장합니다.

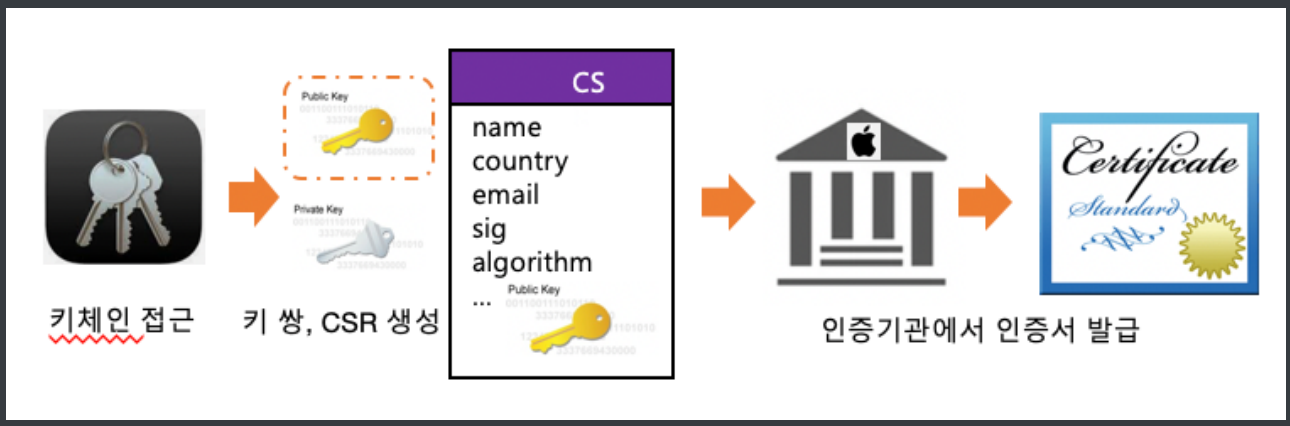
  예시로 대학 또는 전문과정을 마치면 인증서를 받습니다. 인증서는 그 과정을 마쳤고 지식이 있다는 것을 신뢰하는 자료입니다. 인증서는 신뢰받는 기관이 증명하면 더 강력해집니다. 사람들이 해당 인증서를 더 신뢰하기 때문입니다.

  기본적으로 iOS와 Apple의 세계에서도 동일한 개념을 가지고 있습니다. 애플 개발자 멤버쉽에 비용을 지불하고 가입한 합법적인 앱 개발자에게 애플이 증빙하는 인증서를 발급합니다.

  인증서는 iOS 코드서명에 대한 핵심 내용입니다.

- **인증서 발급**

  공개키 인프라 시스템에서 csr은 기본적으로 인증서를 신청하기 위해 사용자가 인증서 기관에게 보내는 메시지이며 애플은 인증서를 발행 하기 위해서 csr 형태의 메시지를 받아서 세부정보를 확인 후 애플의 서명이 포함된 인증서를 발급합니다. (아래에 단계적으로 설명)



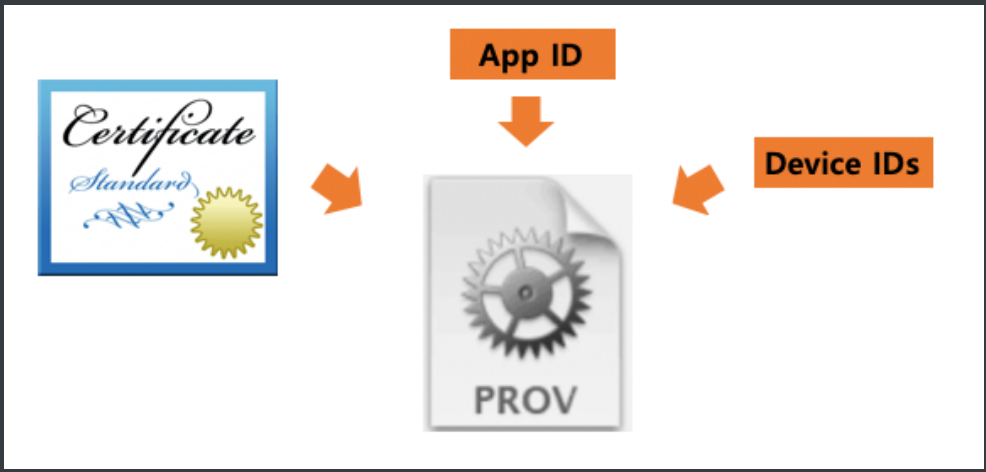
- 키체인 접근 (키 관리 클라이언트)
- 신청자는 인증기관에 인증서 요청 (certificate signing request)
  - 키쌍 생성 후 세부정보 입력(이름, 이메일, 국가)과 서명과 함께 공개키 제출
    - 개인키를 바탕으로 CertificateSigningRequest.certSigningRequest (세부정보, 공개키 포함) 생성
    - 키체인에 개인키는 저장됨
- 해당 인증서 요청전문(csr)은 애플 개발자 맴버쉽 프로그램에서 인증서 생성시 사용됨
- 인증서 발급시 발급 기관(애플)은 누가 요청하는지에 대한 세부 정보를 확인하여 인증서를 발급
- 발급 받은 ios_development.cer/ ios_distribution.cer 더블 클릭 시 Apple Worldwite Developer Relations Certification Authority가 서명한 인증서인지 체크하고 키체인에 있는 내 개인키와 인증서가 결합이 되어 xcode에서 사용 가능한 형태가 됨

- **프로비저닝 프로파일 생성**

  Apple의 인증서가 아닌 Apple이 발급한 개발자 인증서로 코드 서명한 앱을 기기에 설치할 때는 프로비저닝 프로파일이 반드시 필요합니다. 프로비저닝 프로파일에 명시된 기기에 프로비저닝 프로파일을 설치해야 Apple의 인증서로 코드 서명된 앱이 아니더라도 기기에서 실행할 수 있기 때문입니다.

  - 프로비저닝 프로파일 또한 개발용/배포용이 있으며 각 인증서와 결합되어 사용됨
  - 생성과정은 아래와 같이 여러 요소와 연관되어 있음
    - Team ID
    - Bundle ID

- App ID
- Device ID
- Entitlements



- **코드 서명**
  - xCode IDE에 내 개인키로 코드 서명 후 바이너리 파일(IPA) 생성
    - iOS 보안 구조 코드 서명
    - 파일의 무결성 검증, 서명자 확인하는 기능
    - Mach-O 형식의 ios 바이너리 파일의 무결성을 검증하고 서명자를 확인 시 code signature 구조체를 이용한다.
  - 앱스토어에서 설치된 앱은 apple에서 발급한 인증서로 코드서명 되어 있다.
  - 개발자가 테스트하거나 배포하는 앱은 apple이 발급한 개발/ 배포 인증서로 코드서명 한다.

- 참조
  - https://engineering.linecorp.com/ko/blog/ios-code-signing/

4강 푸시 (Push)

- Push
  - APNS (Live coding)
    - Apple push notification service
    -
  - FCM (Live coding)
    - Firebase Cloud Messaging