iOS签名证书及加密 (NXB.19Q3)

- 数字签名
  - 前端签名流程
    - 1:待传输的数据(D)
    - 2:通过HASH算法，得到数据(D)的HASH值(D-H)
    - 3:对HASH值(D-H)进行非对称加密(RSA),得到(D-H-R)
  - 前端-> 数据(D)和(D-H-R) -> 一并传给服务器
  - 后端签名的验证
    - 1:通过HASH算法，得到数据(D)的HASH值(D-H)
    - 2:通过私钥解密签名文件(D-H-R)得到(D-H-1)
    - 3:比较(D-H)和(D-H-1)是否相同
      - 相同:合法
      - 不相同或者解密失败:不合法
- 代码签名
  - 将开发者上传的APP代码进行上述[数字签名]流程
    - 作用->区别官方还是盗版或者病毒软件
- 双重签名（双层代码签名）
  - 申请CSR文件
    - 1:苹果电脑系统(公钥M + 私钥M)
    - 2:从证书颁发机构申请CSR文件 (公钥M)
    - 4:CSR文件
      - 包含设备信息,设备id,APP id等等
      - 包含权限信息等等
      - 包含证书:私钥A 对 公钥M 进行签名
    - 3:苹果服务器(私钥A) 返回CSR文件
  - 描述文件
    - 1:开发前注册苹果开发者账号->支付99/299美元购买发布/安装服务 -> 登录developer.apple.com
    - 2:创建应用(标识唯一Bundle ID :比如xxa.xxxb.com) ,-> 上传CSR文件, ->上传用户手机UDID唯一标识 -> 创建证书
    - 3:下载证书描述文件到电脑- > 双击安装, -> 然后打开‘‘钥匙串’’,找到证书, -> 展开:包含一对公私钥(‘专用密钥’就是私钥,可导出的P12文件,三方平台类似极光推送需要P12文件)
    - 4:描述文件分为 真机和模拟器
  - IPA包
    - 1:Xcode创建项目开发
    - 2:选择开发者账户,选择自动获取证书,编译项目
    - 3:导出ipa包
      - 可执行文件MachO和framework, 图片等静态资源等等
      - 描述文件(服务器私钥A加密的证书)也一并会打包到项目中
      - 对于企业版APP需要信任描述文件(xxx.mobileprovision)才能安装, 而App Store下载的不需要
      - 私钥M 对 代码文件进行签名(ipa就是代码文件夹的压缩包)
    - 4:上线App Store
      - 服务器私钥A解密证书-> 校验代码文件合法性 -> 审核 -> 上线
    - 5:苹果手机安装
      - 手机系统包含的公钥A解密证书-> 校验代码文件合法性 -> 安装使用
    - 6:iOS APP安装源
      - App Store : 所有苹果手机可登陆下载
      - ipa包 (99证书) : 开发者添加过的手机才能安装, 内部测试
      - ipa 包 (299企业证书): 限制手机数量可安装,需要信任描述文件,无需绑定手机
      - 越狱应用