河南青云信息技术有限公司

iPhone数字签名和签名标识

- 代码签名确保代码的真实以及明确识代码的来源
- 苹果公司在发布每一个应用程序前也都要添加他自己的数字签名

为什么要有代码数字签名?

- 苹果要求所有的iPhone应用程序都需要使用苹果提供给已注册的iOS开发者的签名许可进行数字签名，这个签名证明了该应用程序开发者的身份以及确保这个应用程序在签名以后没有被修改或者篡改过。
- 数字签名使用众所周知的公有密钥和私有密钥的算数关系加密术。私有密钥使用在签名的过程中，公有密钥来验证这个签名的有效性， 公有签名被存储在签名证书中，而私有密钥被单独的存储 ,这种证书和算数加密结合的私有密钥叫做数字标识或者签名标识。

如何获取iOS开发签名标识

- 在Keychain Access utility 里边的Certificate Assistant创建一个签名许可请求（CSR），通过这个请求从苹果开发者服务器上得到iPhone开发者计划的计划入口的正式许可。当请求被正式批准后，下载这个证书，双击安装这个文件，就可以将其安装到keychain中，在生成签名许可请求(CSR)的过程中，会自动生成一对公有-私有密钥，它包括发送给苹果的许可请求中的公有密钥（public key）和存储在keychain中的私有密钥，当下载安装签名许可的时候，Keychain Access utility 将其与私有密钥关联，以创建签名标识。（我们可以打开Keychain Access utility，点击Category面板下的My Certificates 以察看许可的关联私有密钥。当安装了已签名的应用程序到iPhone上的时候， iOS将要验证签名以确保该应用程序已签名，并且签名以后未被篡改。如果签名无效或者根本就没有签名，iOS将不允许该就算程序运行。同样，当提交应用程序给苹果审批和部署的时候，首先必须用自己的签名标识为应用程序签名，同时随程序一起提交签名证书（私有密钥不用提交到苹果），然后苹果验证该程序代码是否来自有效的已注册的开发者。最后，苹果用她自己的签名证书为你的已签名的应用程序签名，然后你的应用程序才能在iPhone等苹果设备上正常的运行。

基本概念

- 所有的iPhone应用程序在iOS设备上运行之前必须用合的signing identity(签名标识)进行签名。
- 为了在自己的iOS设备*开发*而做应用程序签名，需要:
    - 私钥
    - iPhone 开发者证书

    - Development Provisioning profile
- 为了让自己的开发的应用程序发布在AppStore，需要：
    - 私钥
    - iPhone Distribution 证书
    - AppStore Distribution Provisioning profile
- 为了让自己的应用程序在Ad Hoc上，需要：
    - 私钥
    - iPhone Distribution证书
    - Ad Hoc Distribution Provisioning profile

私钥是在生成认证签名请求(CSR)时创建的， 在CSR提交和通过后，可以在iPhone Developer Program Provisioning Portal里创建和下载证书以及provisioning profiles.

Signing identity (签名标识) 由私有加密key 和数字证书组成，在iOS开发中， XCode 用私钥来签署程序，这样程序就可以在iOS开发设备上运行或者提交到App Store上。 公钥包含在iOS开发者/发布证书，用来认证已签名的程序。 Provisioning profiles 用来告知XCode用哪个证书/私钥组合来签署程序，开发设备也通过它来决定如何认证安装在设备上的程序。