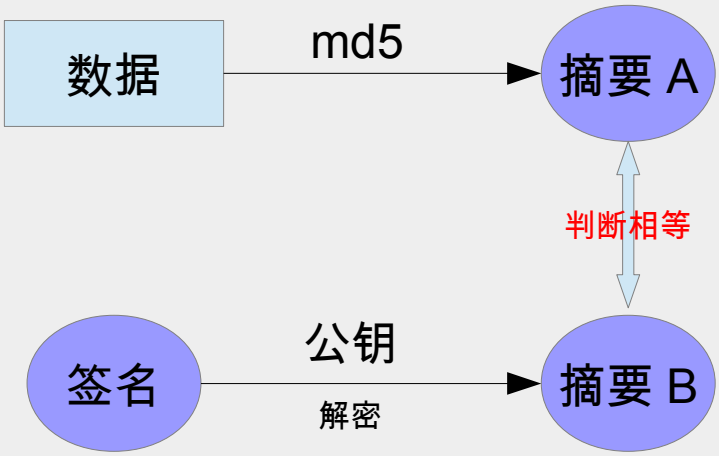
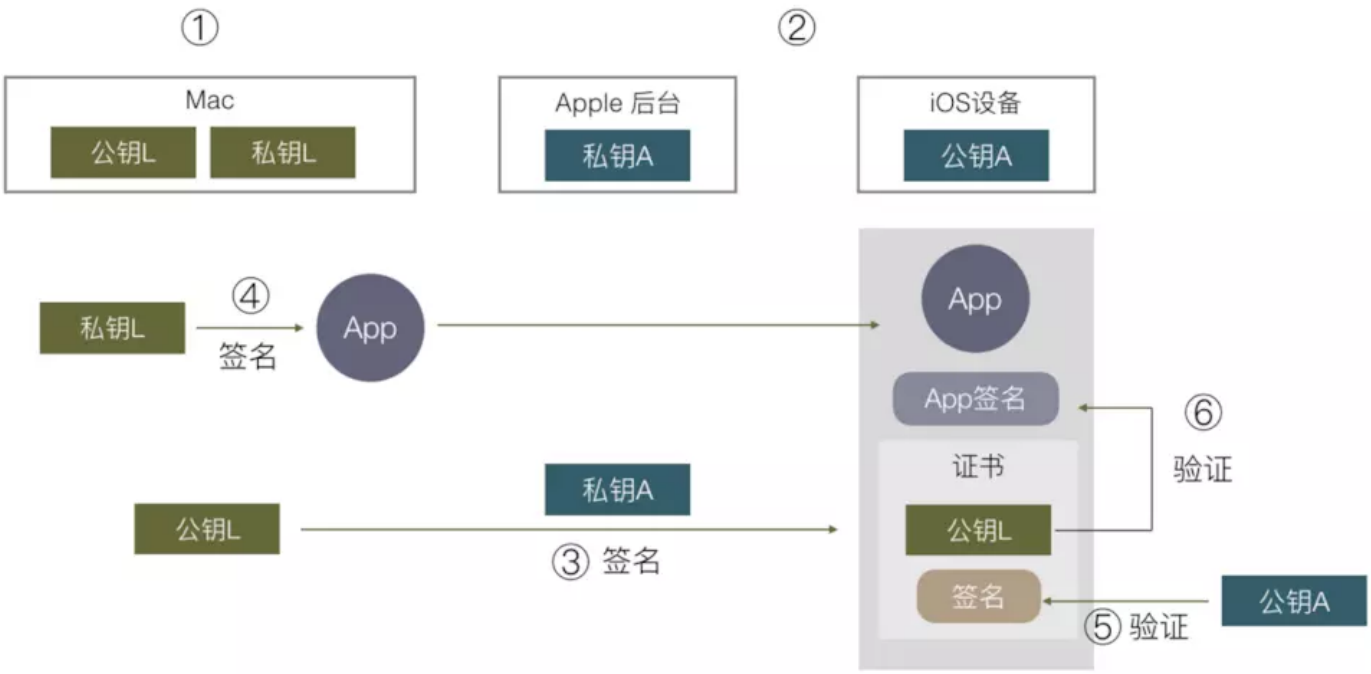
数字签名

私钥只是对摘要加密，并不会对数据进行加密

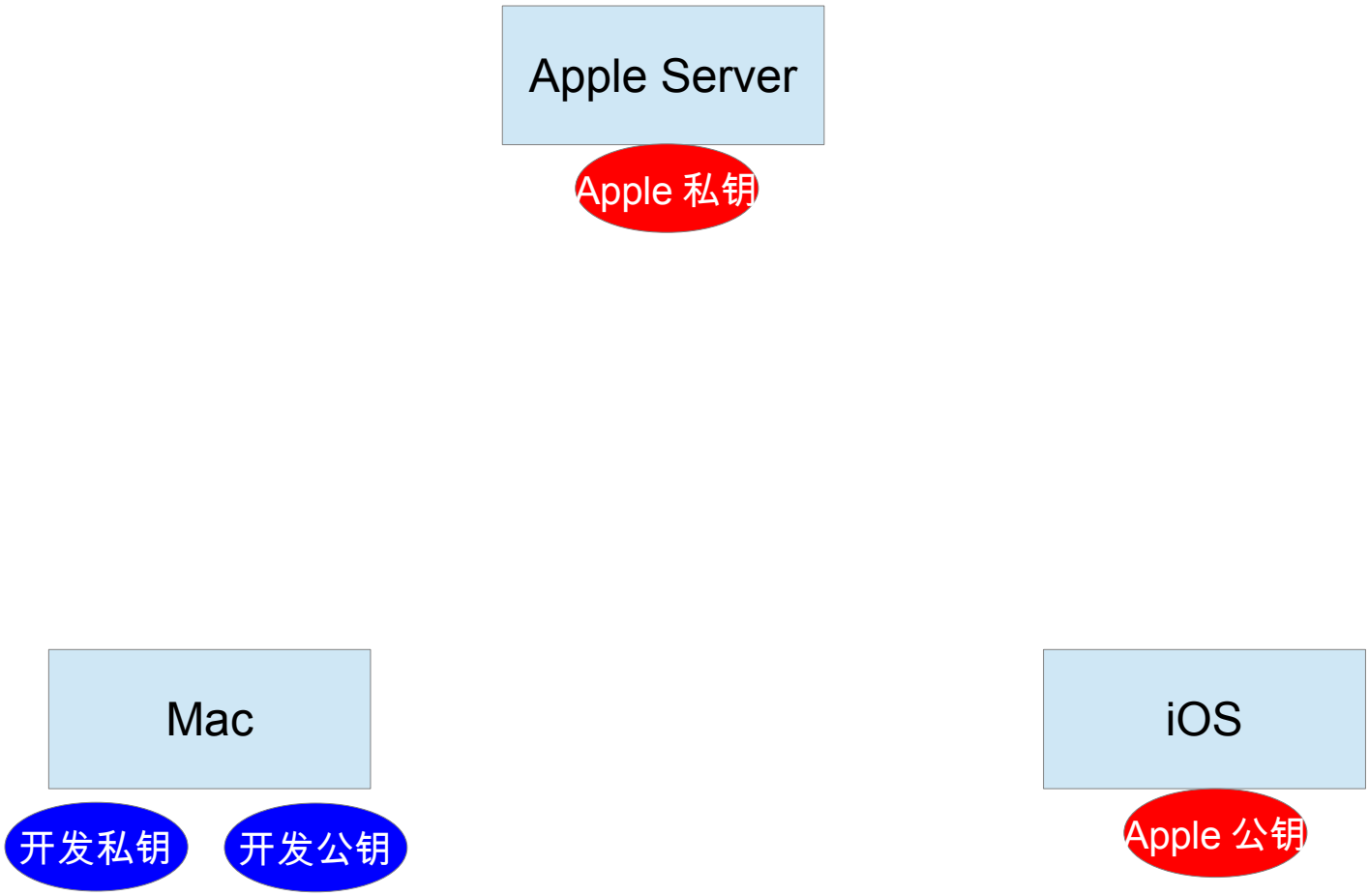


如果摘要 A== 摘要 B ，那么数据是没有被篡改过的。

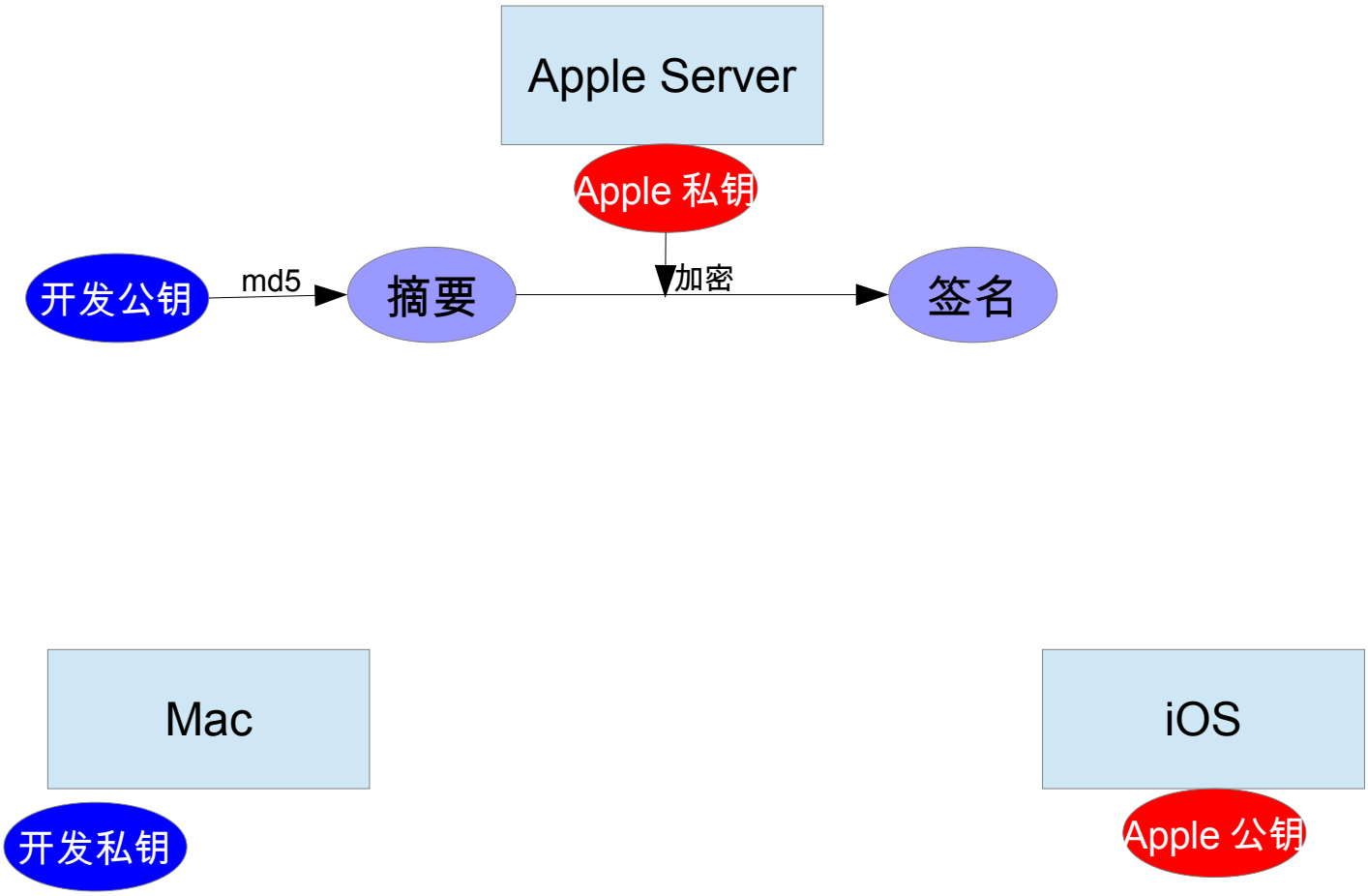
开发证书


①
②
Mac
公钥L
私钥L
Apple 后台
私钥A
iOS设备
公钥A
私钥L
④
签名
App
App
App签名
⑥
验证
证书
公钥L
私钥A
公钥L
③ 签名
签名
公钥A
⑤ 验证

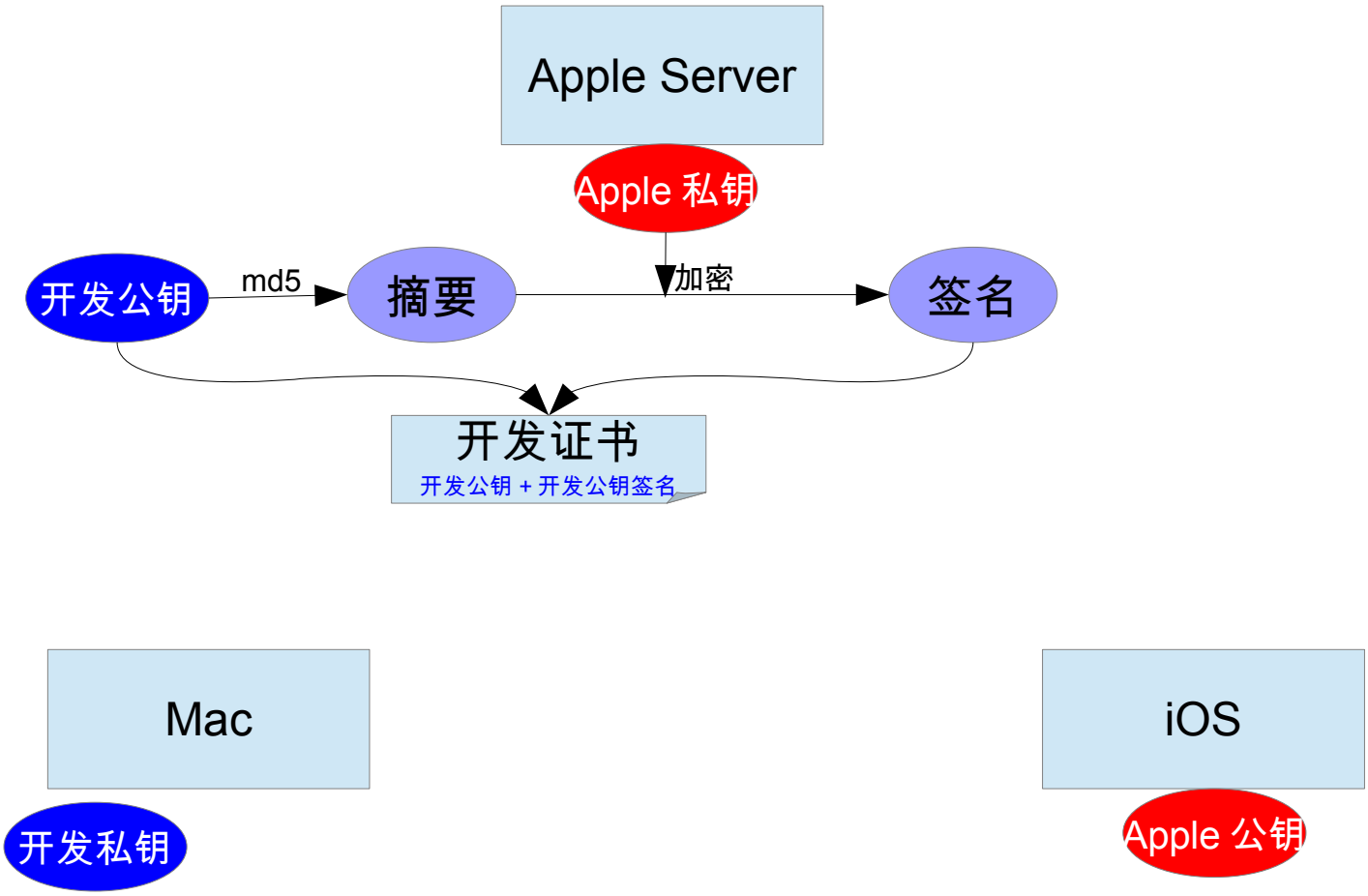
开发证书



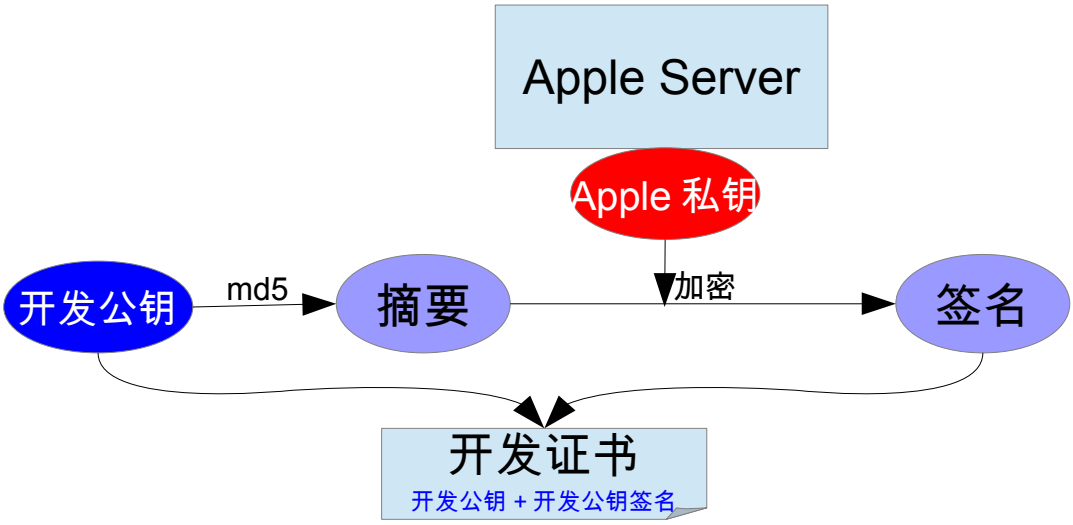
开发证书



开发证书

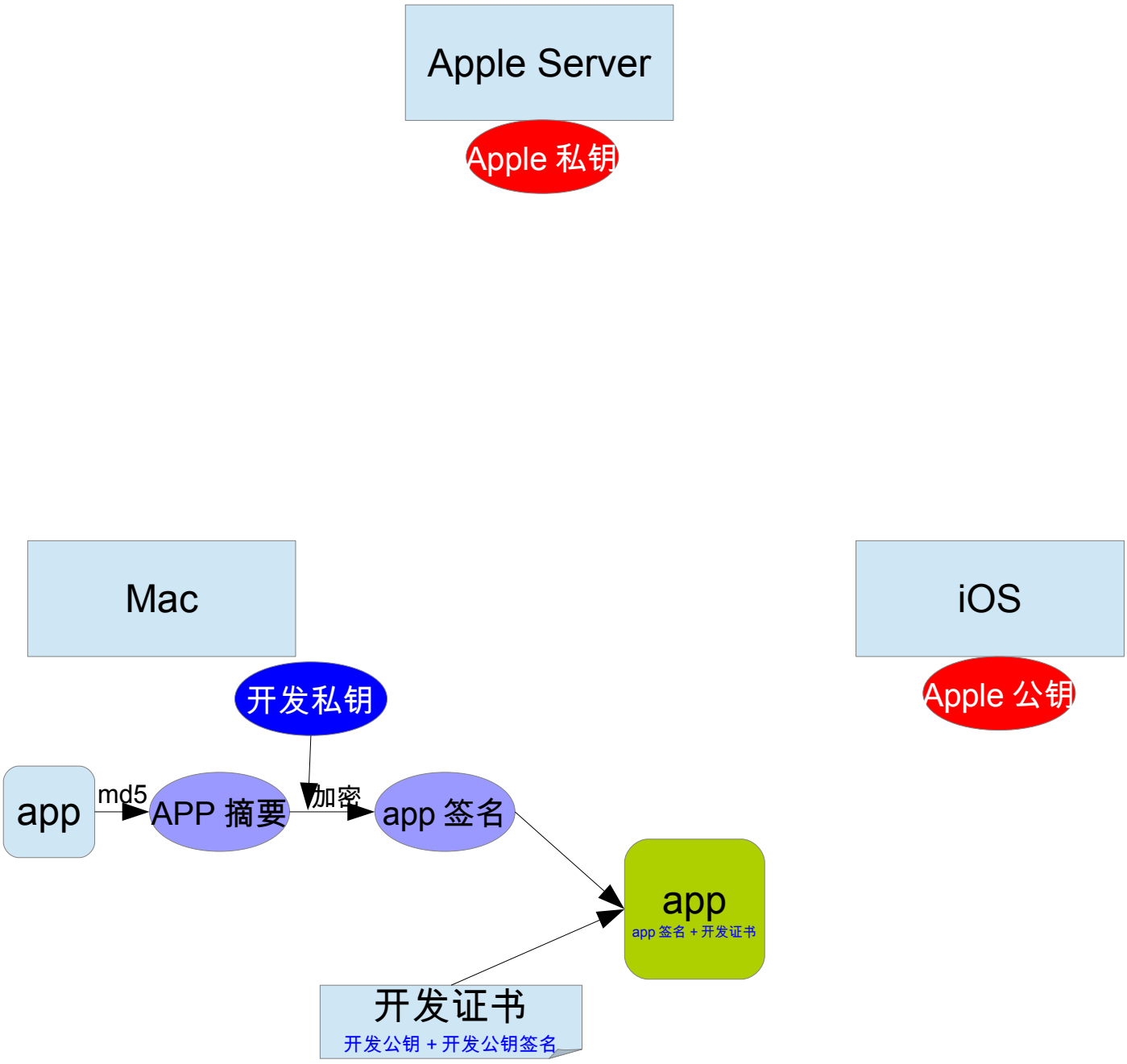

Apple Server
Apple 私钥
开发公钥
md5
摘要
加密
签名
开发证书
开发公钥 + 开发公钥签名
Mac
开发私钥
iOS
Apple 公钥

开发证书

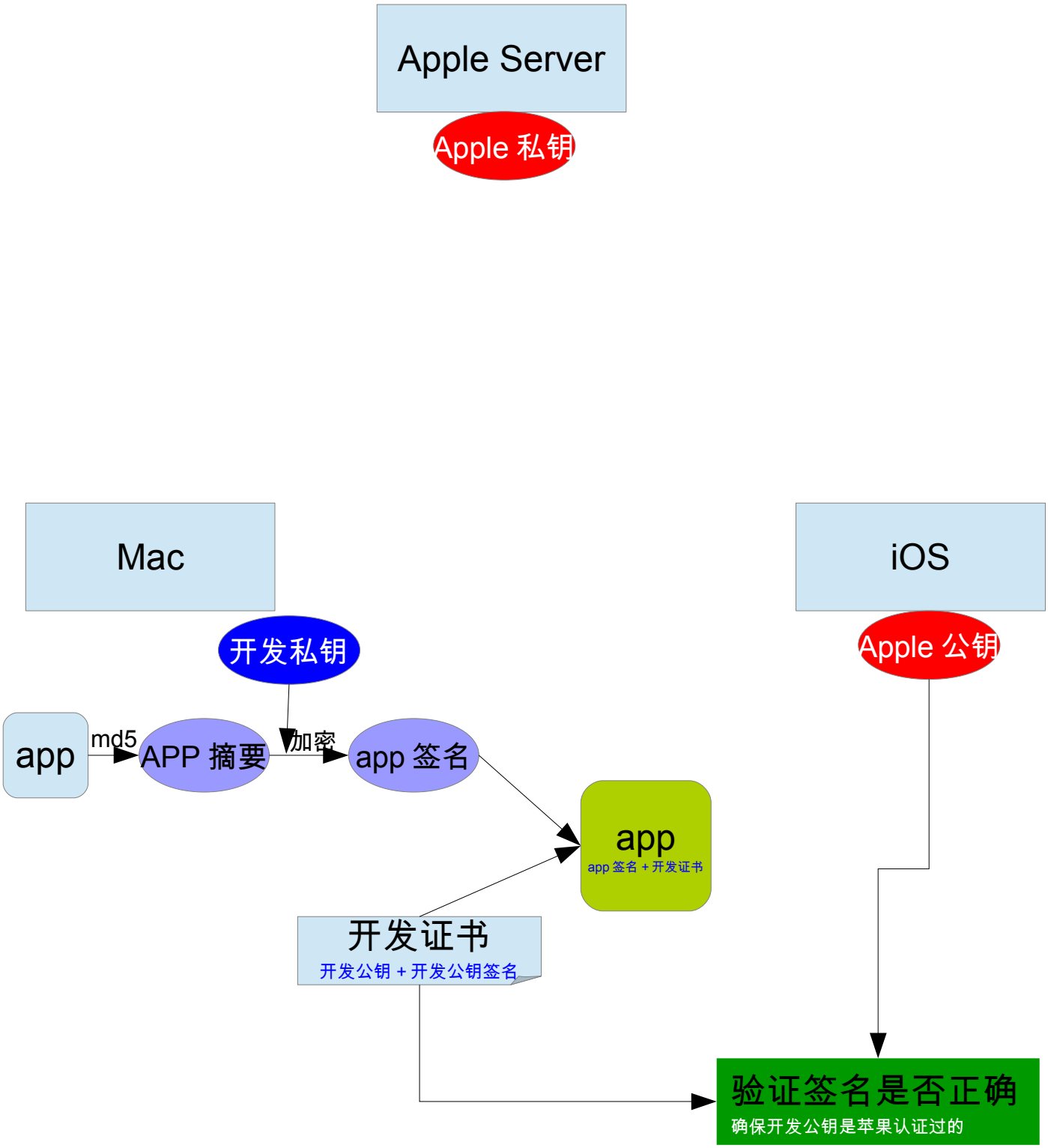

Apple Server
Apple 私钥
开发公钥
md5
摘要
加密
签名
开发证书
开发公钥 + 开发公钥签名


Mac
iOS
开发私钥
Apple 公钥
app
md5
APP 摘要
加密
app 签名

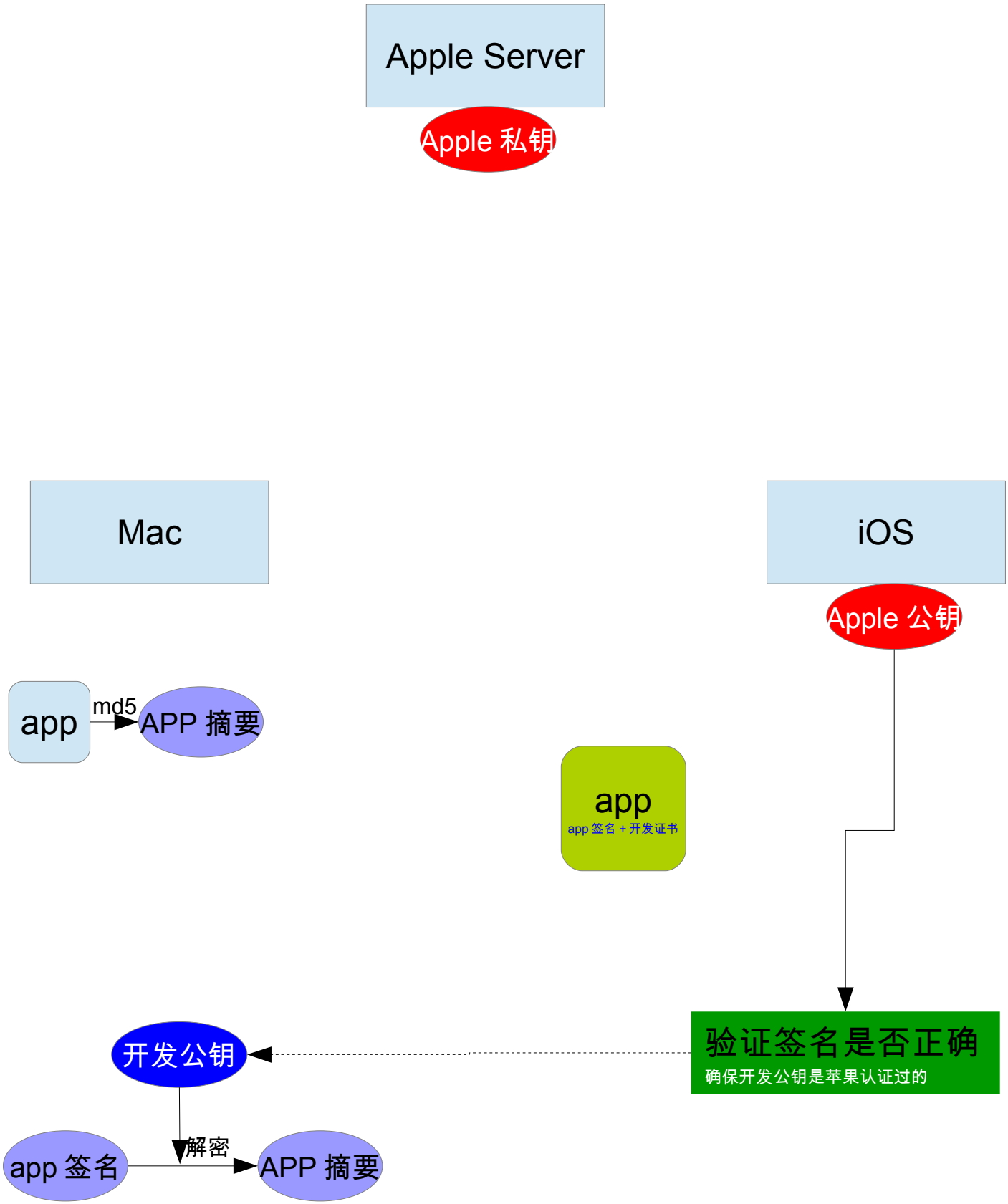
开发证书


Apple Server
Apple 私钥
Mac
iOS
开发私钥
Apple 公钥
app
md5
APP 摘要
加密
app 签名
app
app 签名 + 开发证书
开发证书
开发公钥 + 开发公钥签名

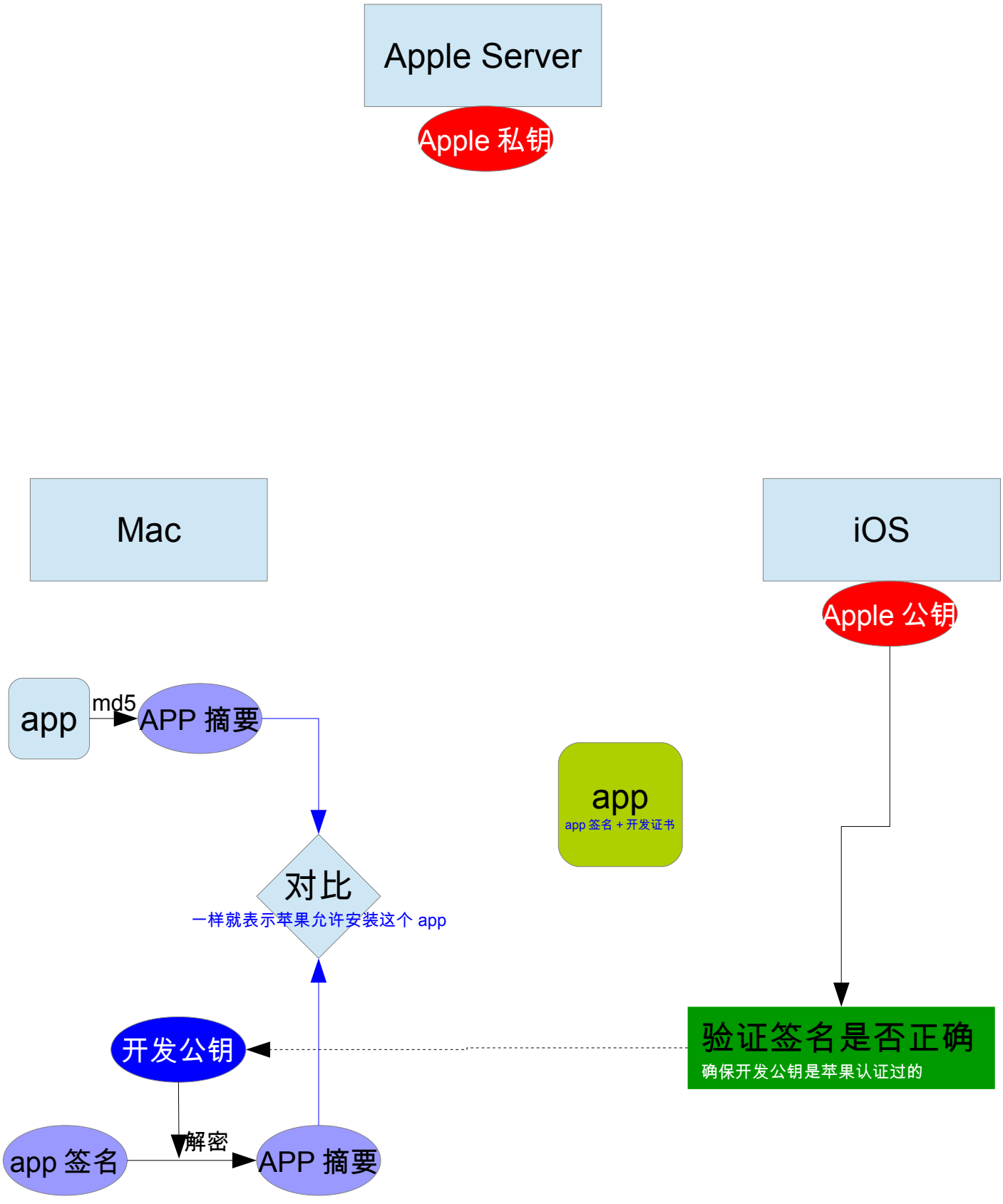
开发证书


Apple Server
Apple 私钥
Mac
iOS
开发私钥
Apple 公钥
app
md5
APP 摘要
加密
app 签名
app
app 签名 + 开发证书
开发证书
开发公钥 + 开发公钥签名
验证签名是否正确
确保开发公钥是苹果认证过的

开发证书

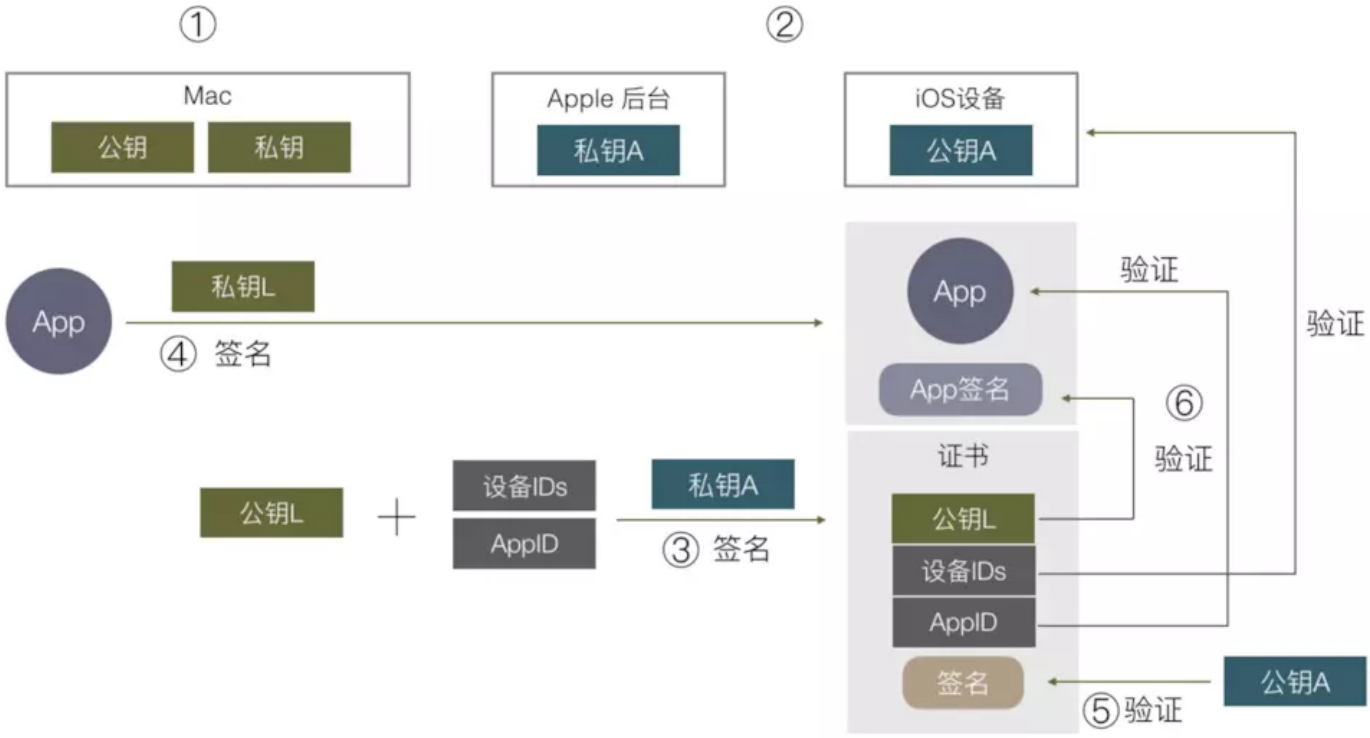

Apple Server
Apple 私钥
Mac
iOS
Apple 公钥
app
md5
APP 摘要
app
app 签名 + 开发证书
验证签名是否正确
确保开发公钥是苹果认证过的
开发公钥
app 签名
解密
APP 摘要

开发证书


Apple Server
Apple 私钥
Mac
iOS
Apple 公钥
app
md5
APP 摘要
app
app 签名 + 开发证书
对比
一样就表示苹果允许安装这个 app
开发公钥
验证签名是否正确
确保开发公钥是苹果认证过的
app 签名
解密
APP 摘要

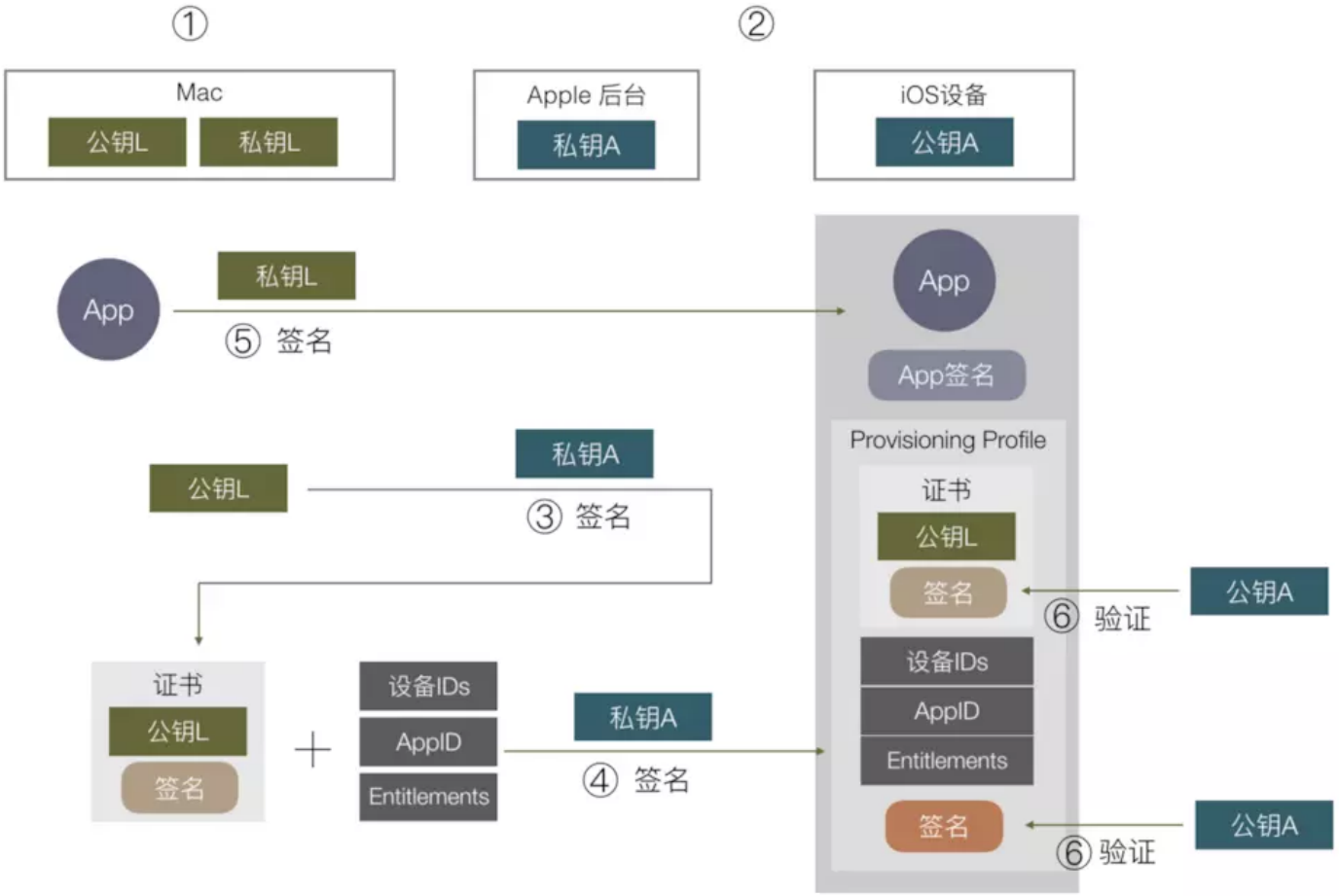
开发证书

避免被滥用，苹果加了 2 个限制：一是在苹果后台注册的设备才可以安装；二是限制签名只能针对某一个具体的 APP 。



开发证书

苹果想控制其他权限，例如： iCloud 、 push 、后台运行等，把这些权限开关统一称为 Entitlements ，也是需要通过签名授权。



开发证书
开发公钥 + 开发公钥签名

+

AppID
设备 IDs
Entitlements

=

Provisioning Profile

打包进 app ，文件名为：

embedded.mobileprovision

掉签

企业签名掉签后的用户端的情形

首先在掉签之后，新用户会无法下载，在下载之后，APP只显示名称，而不显示正常的图标，同样在"描述文件与设备管理"中，不会出现新的“企业级应用”。

这里需要注意的是，在分发平台不稳定时，也会出现下载失败，而这种情况表现为：一直处于"等待中"，或者提示下载失败，需要特别注意。

已经安装的用户会无法打开应用，提示"未受信任的企业级开发者"，并且我们打开"描述文件与设备管理"，找到对应证书后，点击"验证应用"无法通过， 这就表示该APP所签的签名已经掉签。

掉签