



第三届 全国网络与信息安全防护峰会

对话·交流·合作



基于第三方认证的安卓应用管控机制

郑辉

网秦安全技术总监

主要内容



1 安卓应用治理现状

2 数字签名证书体系

3 安卓应用数字签名

4 第三方认证方案

安卓应用治理现状



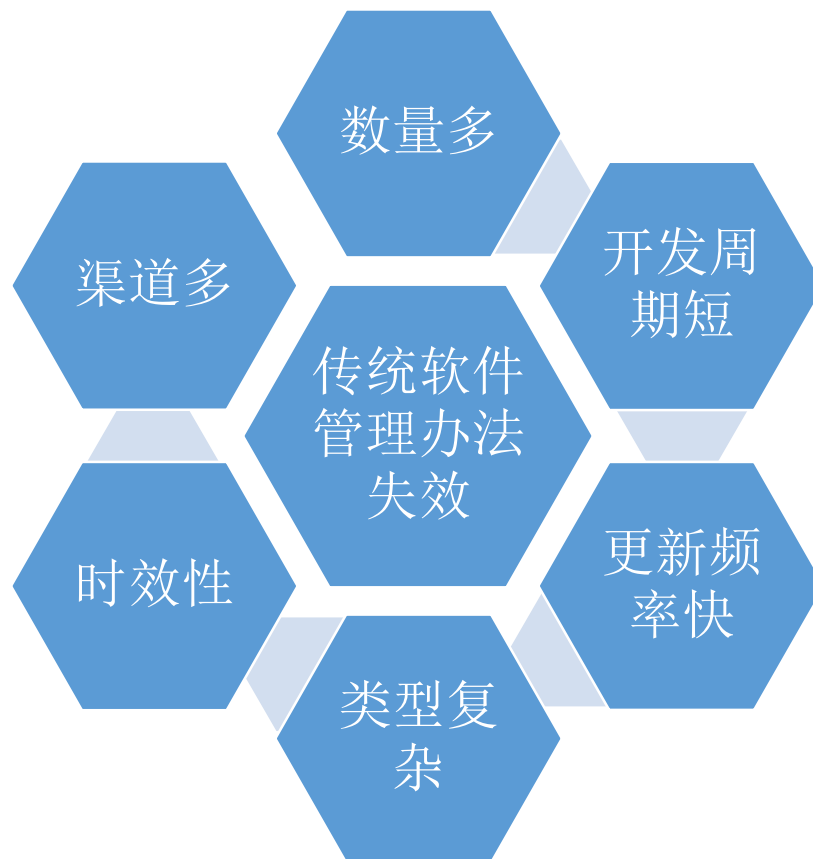
安卓应用治理面对的问题

多方重视

工信部指导意见

核心支持技术

安卓应用治理现状-问题(1)



安卓应用治理现状-问题(2)



安卓应用治理现状-多方重视



- 中央网信办
 - 10月25日，中央网信办主任鲁炜在推进网络空间法治化的座谈会上透露，国家网信办将出台App应用程序发展管理办法
- 工信部通信保障局、电信研究院
 - 10月24日，中国互联网协会反网络病毒联盟、电信终端测试技术协会、电子认证服务产业联盟在京组织召开移动互联网应用程序开发者第三方数字证书签名与验证试点宣介会。
- 公安部十一局
- 中国互联网协会移动互联网工作委员会
 - 11月27日“2014移动互联产业发展与网络信息安全研讨会”

安卓应用治理现状-指导意见



- （六）加强移动应用商店和应用程序安全管理。
 - 移动应用程序开发者真实身份信息验证
 - 应用程序安全检测
 - 恶意程序下架
 - 恶意程序黑名单
 - 用户监督举报
 - 移动应用程序第三方安全检测机制。
 - 移动应用程序开发者第三方数字证书签名和应用商店、智能终端的签名验证和用户提示机制。
 - 移动恶意程序举报受理和黑名单共享机制。
 - 加强社会宣传，引导用户从正规应用商店下载。

安卓应用治理现状-核心技术



- 对开发者的验证
 - 公钥证书
- 对应用的验证
 - 数字签名

数字签名证书体系



数字签名原理

时间戳原理

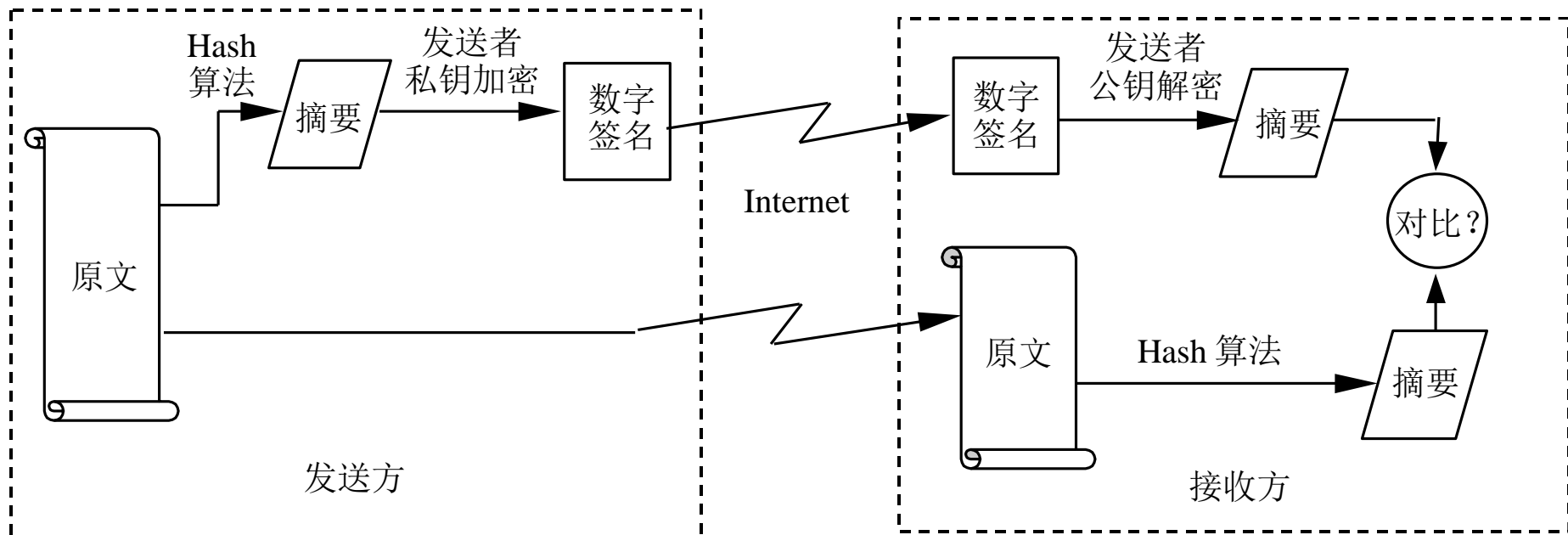
CA (Certificate Authority)

X.509证书格式

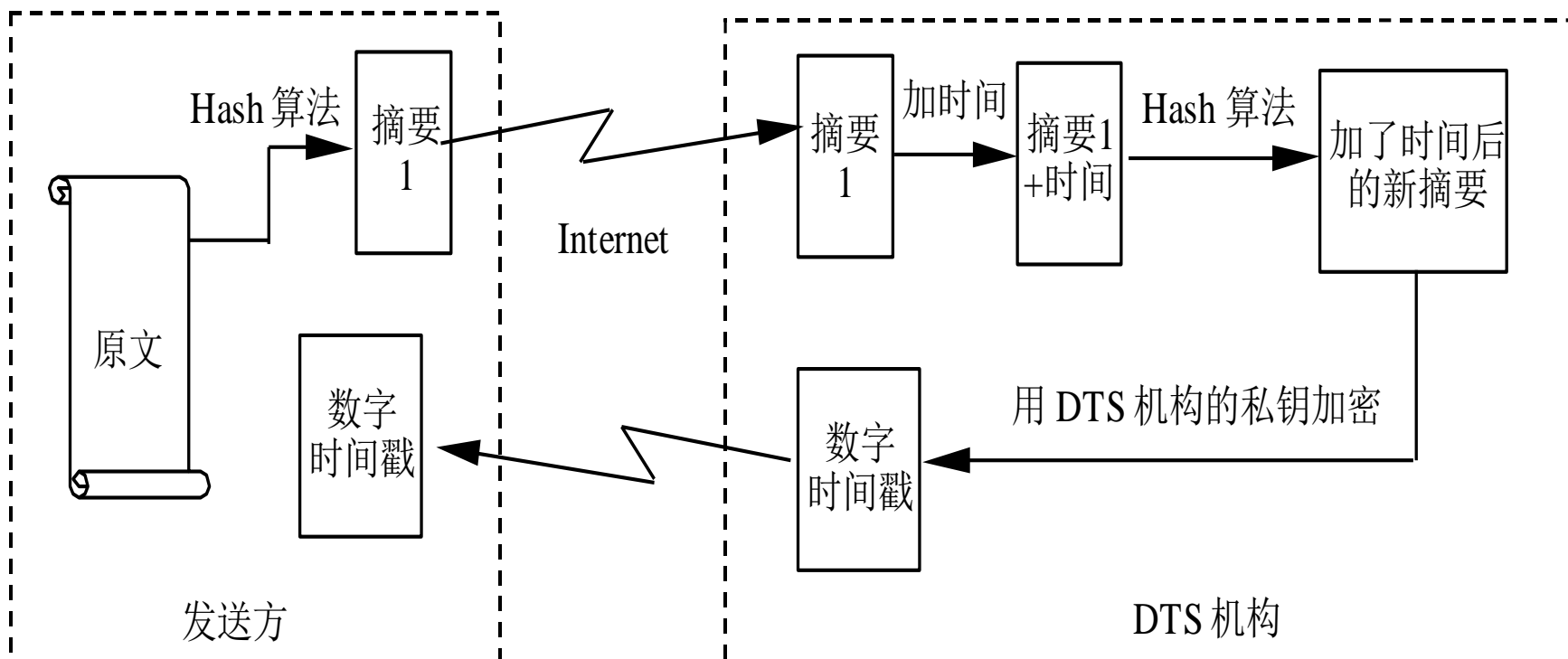
PKI (Public Key Infrastructure)

PKCS #7 #12

数字签名证书体系-原理



数字签名证书体系-时间戳

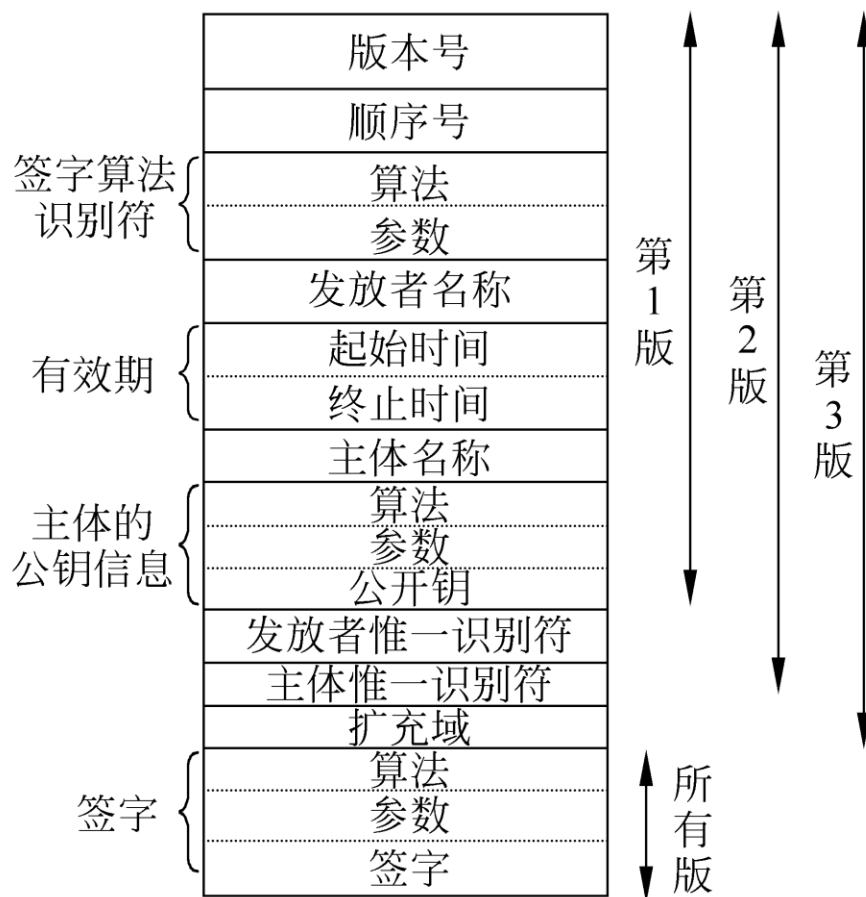


数字签名证书体系-CA

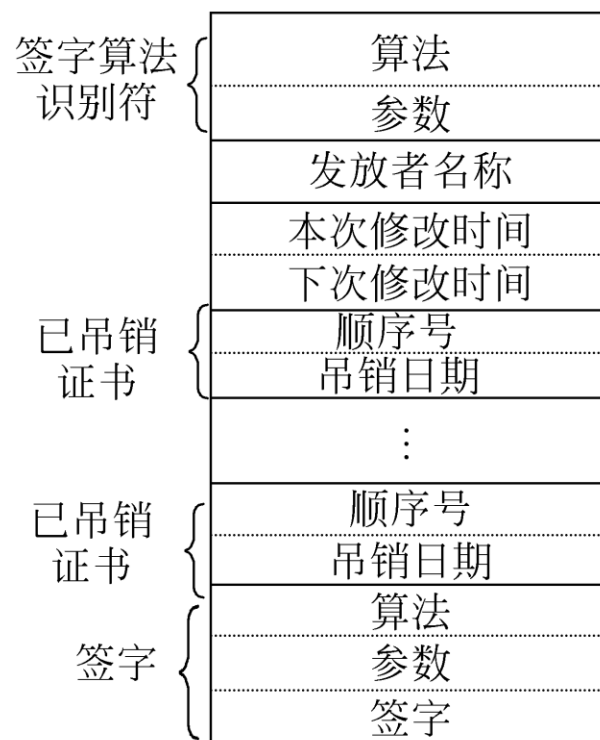


- 为公钥提供担保;
 - 证明各实体在网上身份的真实性;
 - 为各个实体颁发电子证书;
- 管理证书;
 - 证书申请、证书审批、证书颁发、证书撤消、证书更新、证书的归档

数字签名证书体系-X.509



(a) X.509 证书



(b) 证书吊销列表

数字签名证书体系-PKI



- 中国的CA中心建设从1998年底开始。
 - **第一个电信行业CA**-----CTCA
- 2001年成立中国PKI论坛
 - <http://www.chinapkiforum.org.cn>
- **三类CA中心**
 - **行业性CA中心** 中国金融认证中心(CFCA, <http://www.cfca.com.cn>)
 - **金融：建行、招商、中行、工行、农行、交行**
 - **区域性CA中心**
 - 北京、上海、广东、山东、湖北、安徽CA中心 (<http://www.ahca.org.cn>)
 - **商业性CA中心** 企业创办的认证机构

数字签名证书体系-PKCS#7 #12



- Public Key Cryptographic Standards.
 - #7 Cryptographic Message Syntax
 - #12 Personal Information Exchange Syntax Standard

安卓应用数字签名



安卓应用文件结构;

安卓应用验证存在的问题;

APK验证逻辑;

安卓应用的文件结构



- ZIP->JAR->APK
- APK签名文件在META-INF目录下：
 - MANIFEST.MF，所有文件->SHA1->BASE64。
 - CERT.SF，每个条目->SHA1->BASE64。
 - CERT.RSA，针对CERT.SF的数字签名。

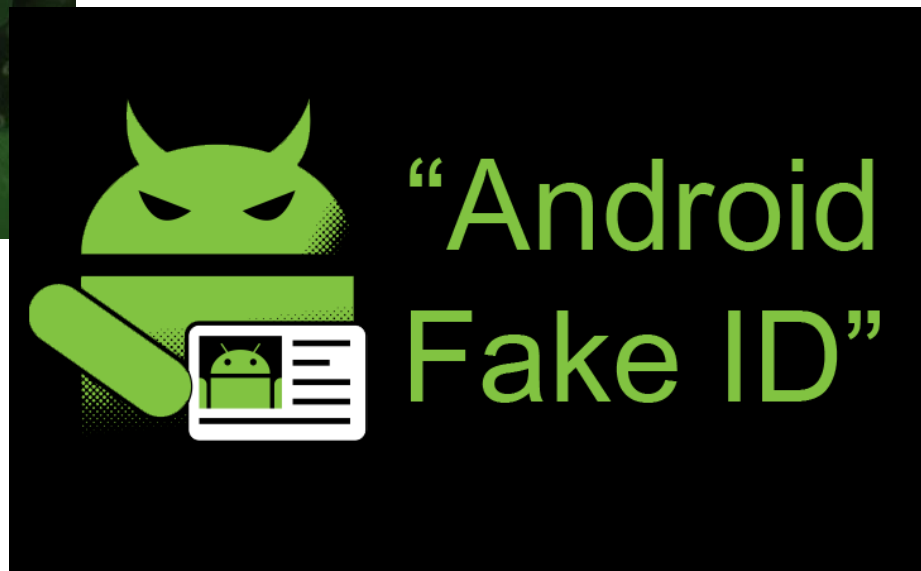
安卓证书验证存在的问题



- MasterKey漏洞
 - BlackHat2013



- FakeID漏洞
 - BlackHat2014



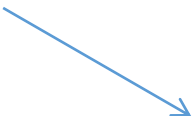
MasterKey漏洞



- APK签名漏洞一：文件名重复添加 #8219321
- APK签名漏洞二：extrafieldlength处理不一致 #9695860
- APK签名漏洞三：主目录文件ExtraLength负数置零 #9695860
- APK签名漏洞四：filenameLength处理不一致 #9950697
- 本质是Zip文件格式解析漏洞；JAVA处理结果和C处理结果不匹配；

- 没有验证证书链的合法性;

```
private static X509Certificate findCert(Principal issuer, X509Certificate[] candidates)
{
    for (int i = 0; i < candidates.length; i++) {
        if (issuer.equals(candidates[i].getSubjectDN())) {
            return candidates[i];
        }
    }
    return null;
}
```



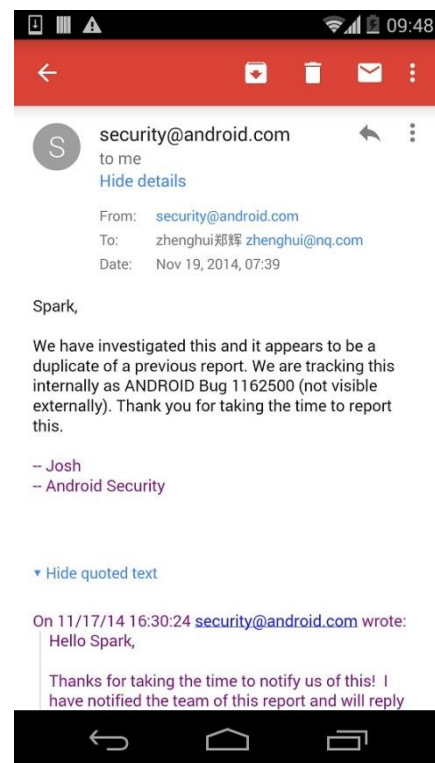
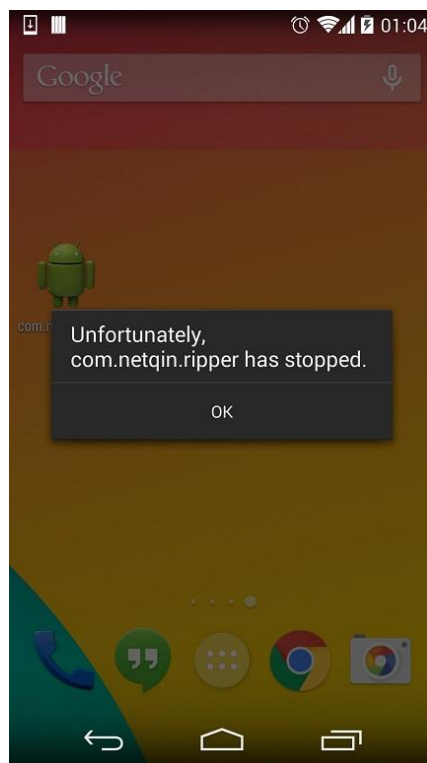
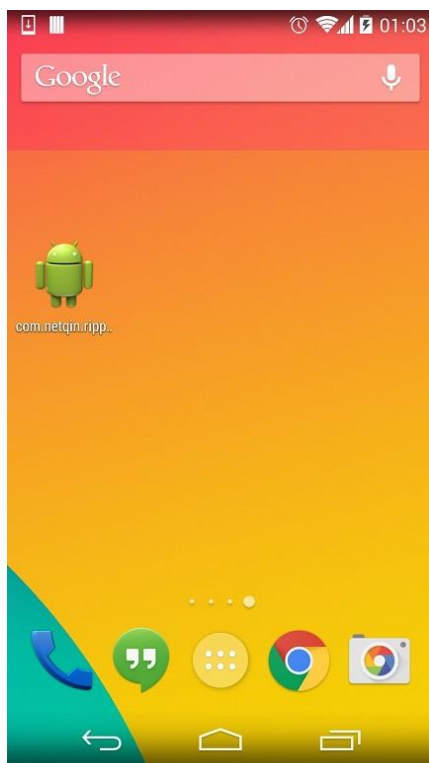
```
private static X509Certificate findCert(Principal issuer, X509Certificate[] candidates,
                                       X509Certificate subjectCert, boolean chainCheck)
{
    for (int i = 0; i < candidates.length; i++) {
        if (issuer.equals(candidates[i].getSubjectDN())) {
            if (chainCheck) {
                try {
                    subjectCert.verify(candidates[i].getPublicKey())
                } catch (Exception e) {
                    continue;
                }
            }
            return candidates[i];
        }
    }
    return null;
}
```

完整性验证漏洞



今天发现Android应用安装时没有做完整性校验，删除包内任意文件仍然可以正常安装，只要保证AndroidManifest.xml和classes.dex这两个文件存在即可。典型的利用方式可以用残缺的高版本应用攻击完整的低版本应用，用户升级后应用就不可用了。Android应用的签名认证体系在实现的时候，真的是千疮百孔啊。

8月4日 15:48 来自 微博 weibo.com



- APK签名文件：
 - META-INF目录
 - MANIFEST.MF, CERT.SF, CERT.RSA。
- META-INF目录下的文件是验证参考，但不作为验证目标。
- META-INF目录下可以添加任意文件。

安卓应用第三方认证方案



基本思路:

- 对APK签署可信第三方数字签名证书;
- 放入APK 文件的META-INF目录下;

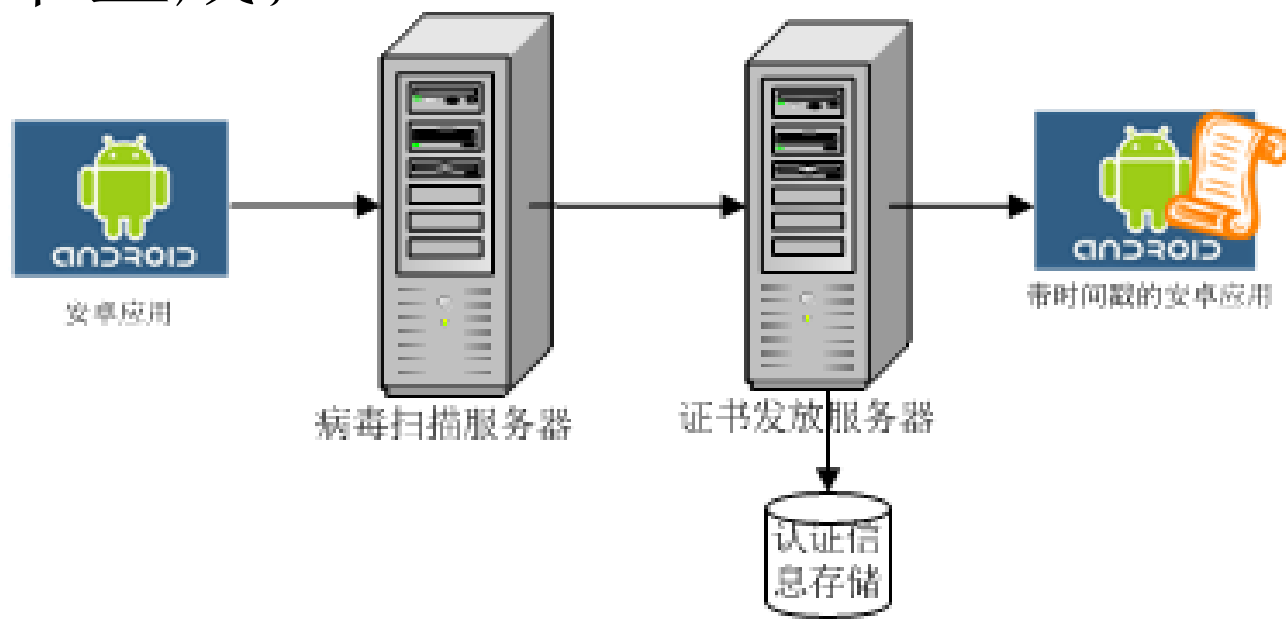
基本步骤:

- 证书生成
- 证书插入
- 证书验证

第三方认证方案-证书生成



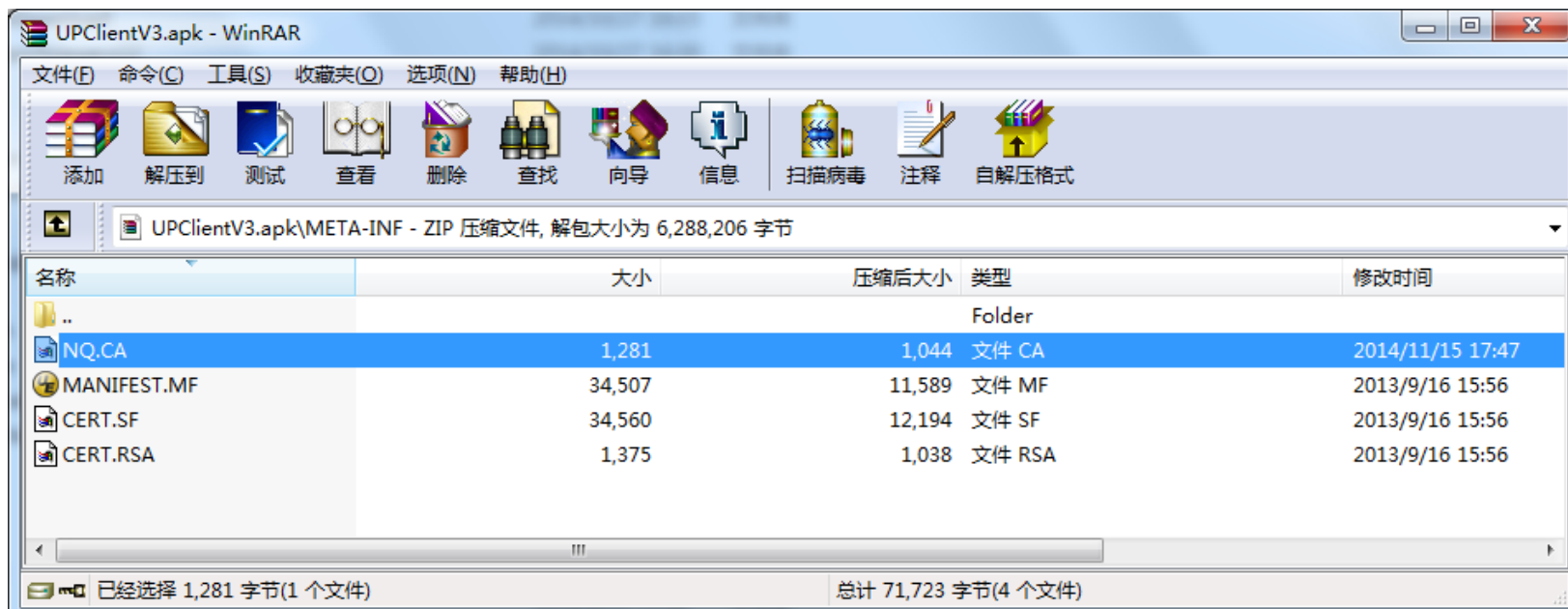
- 应用提交;
- 病毒扫描;
- 摘要信息提取;
 - 多种方案: CERT.SF文件、ZIP文件目录数据块;
- 数字签名证书生成;



第三方认证方案-证书插入



- 追加到安卓应用的META-INF目录;
 - 无需对APK文件解包;
- 服务器端保存;
 - APK文件信息;
 - 证书信息;



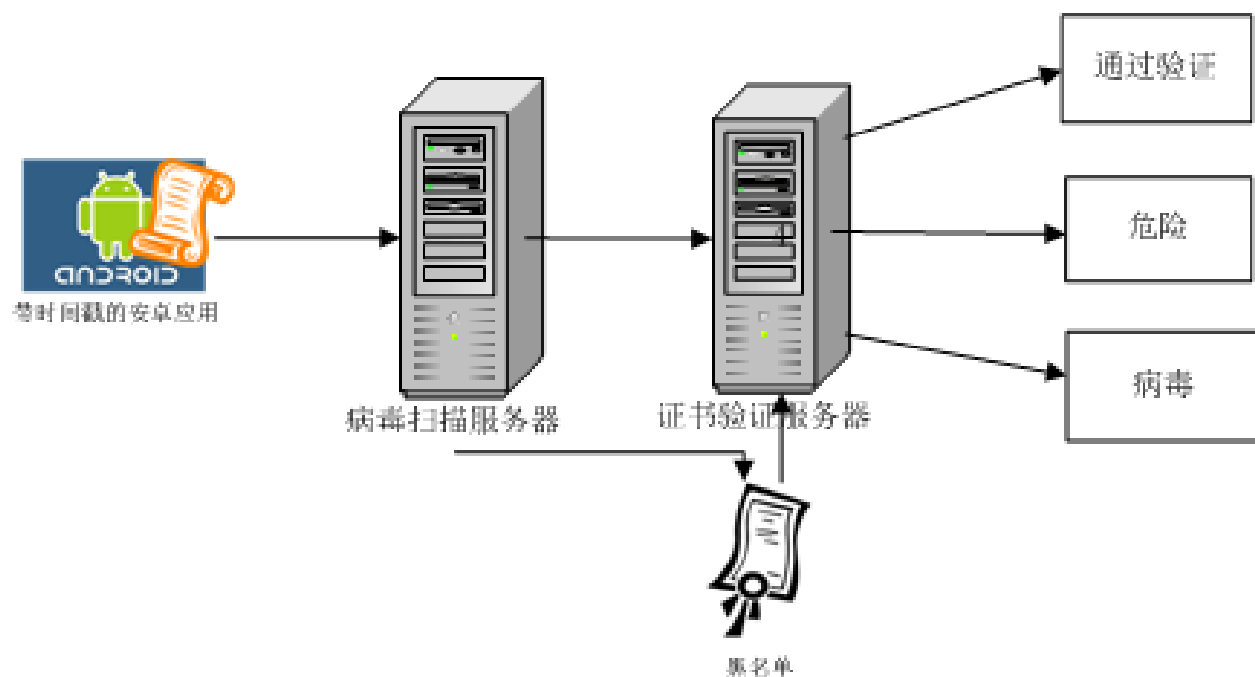
第三方认证方案-证书验证



- 第三方验证;
- 用户端验证;
- 分发渠道/商城验证;

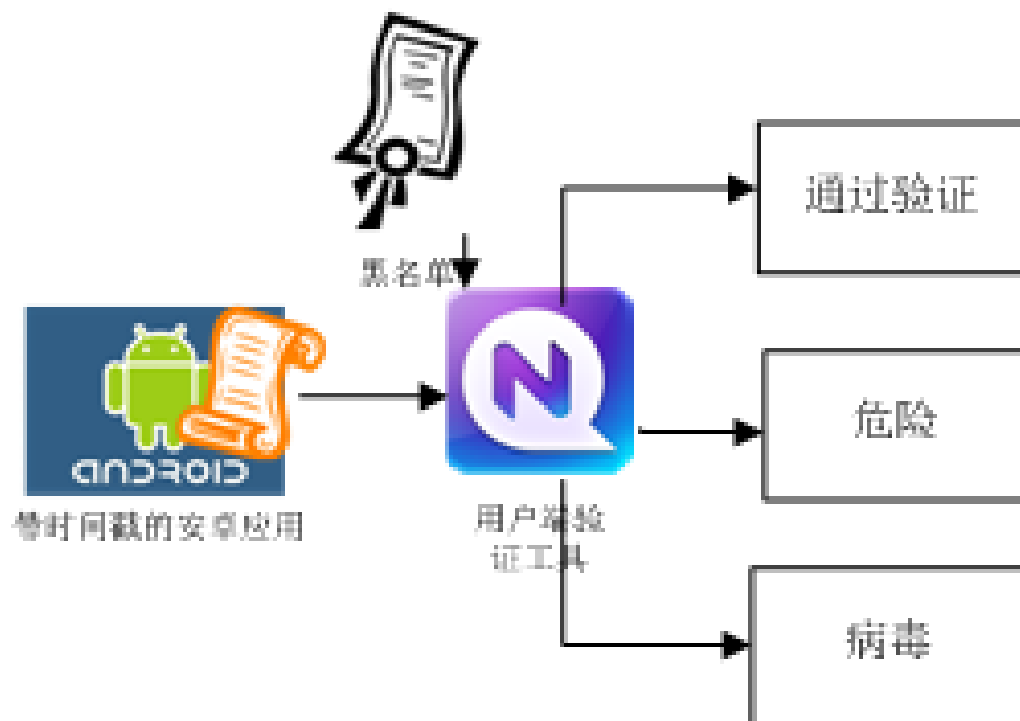
证书验证-第三方

- 应用提交;
- 病毒扫描;
- 证书验证;
- 结果展示;



证书验证-用户端

- 应用下载;
- 证书验证;
- 结果展示;



证书验证-分发渠道/应用商城

Def 2014

- 应用搜集;
- 网络验证;
- 结果展示;



第三方认证方案-优点



- 不依赖安卓系统厂商的验证机制;
- 不影响APK原有（安装、升级）验证机制;
- 可以兼容新老版本APK;
- 技术实现简单;

第三方认证方案-缺点



- 完全依赖第三方对恶意程序的检出能力;
- 数字签名可被删除替换;

- 相比于对开发者管控，对移动应用的管控更具可行性；
- 为移动应用的统一管控提供了技术解决方案；
- 方案推广需要有牵头单位支持；

Q&A

zhenghui@nq.com