

基于分级评估与签名管理的移动应用 可信生态建设

泰尔终端实验室 杨正军

2016年5月30日



■ 移动应用发布渠道众多，市场格局混乱，安全性难以保证

移动应用来源

购机前

操作系统开发商

终端制造商

移动运营商

销售渠道商

预置应用

- 用户购机时已安装
- 一般不能删除

终端厂商缺乏自律，对预置应用疏于管理

恶意吸费

流量消耗

隐私窃取

购机后

应用商店

移动互联网应用

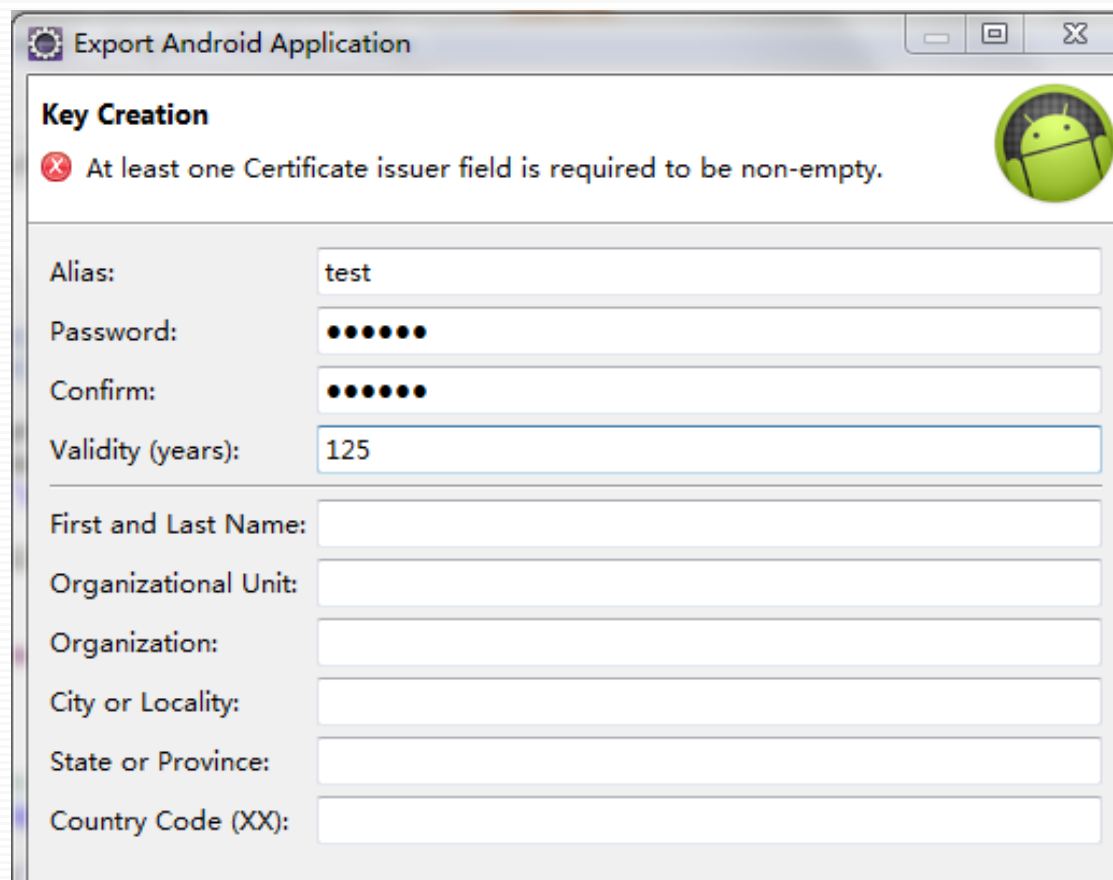
- 用户主动下载安装
- 可自行安装和删除

应用商店审核机制欠缺，对上架应用疏于管理

功能破坏



- 移动终端操作系统（如Android）支持自签名体系，签名混乱，无法溯源



Export Android Application

Key Creation

⊗ At least one Certificate issuer field is required to be non-empty.

Alias: test

Password: ●●●●●●

Confirm: ●●●●●●

Validity (years): 125

First and Last Name:

Organizational Unit:

Organization:

City or Locality:

State or Province:

Country Code (XX):

■ 移动应用管理混乱，移动应用侵犯用户权益

两会提案

- 《关于“重视移动互联网时代的信息应用安全”的建议》（第5099号）
- 《关于加强手机预装软件监督的提案》（3254号）
- 《关于智能手机应保证用户信息安全的提案》（3262号）
- 《关于美国“斯诺登事件”提醒我国应尽快建立智能终端安全保障体系的提案》（3315号）

各地消协

- 《关于规范智能手机预置应用软件保障消费者合法权益的建议》

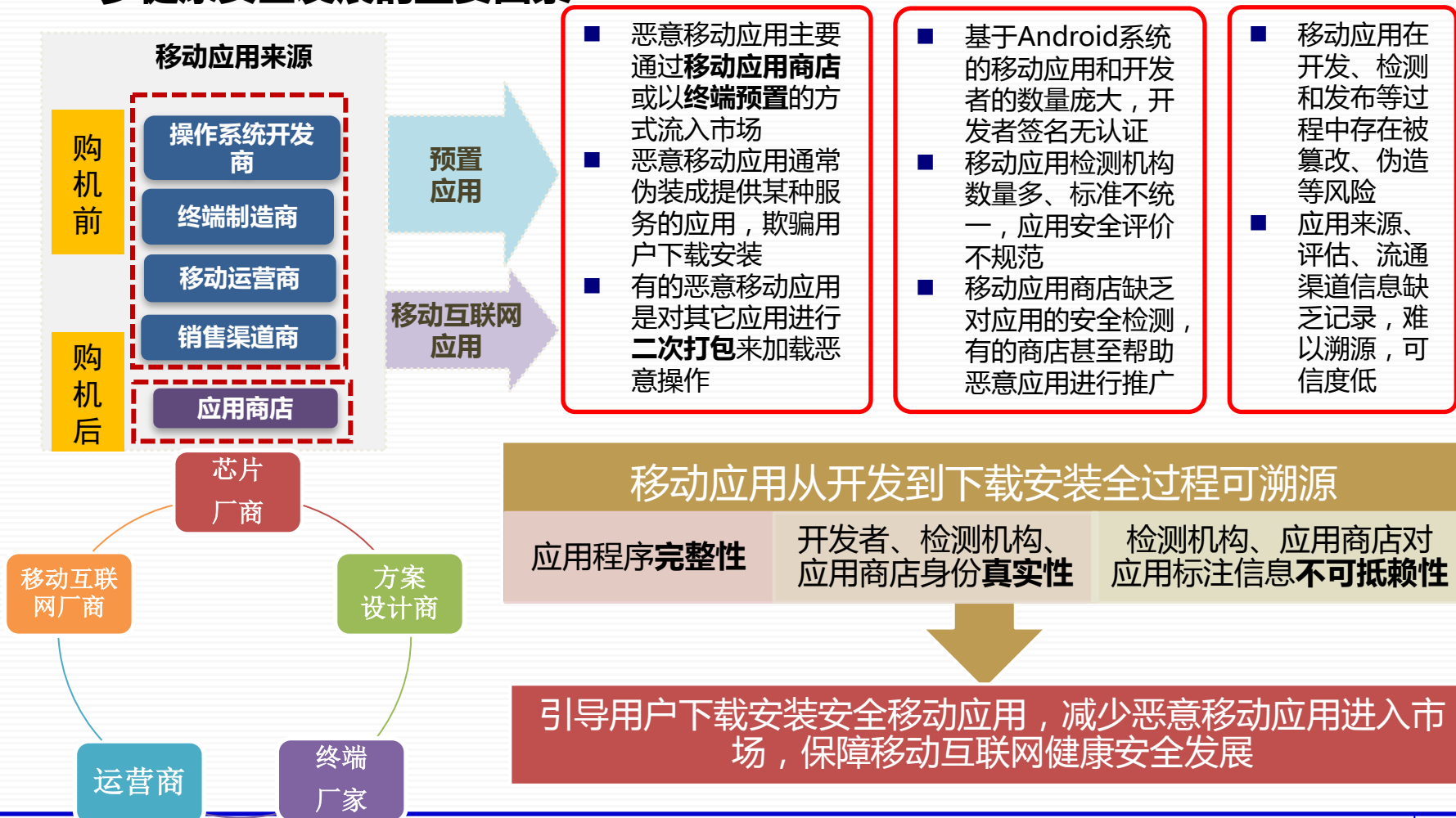
新闻媒体

- 中国中央电视台（CCTV）于2014年3月15消费者权益日晚会曝光高鸿旗下的全自动智能安装软件——大唐神器。2016年3月15号支付软件造成财产损失。
- CCTV[第一时间]手机预装软件合不合法？
- 中央电视台《每周质量报告》2013年10月《我的手机谁做主》曝光手机预装软件内幕
- 中央电视台《每周质量报告》2014年9月《隐私危机》

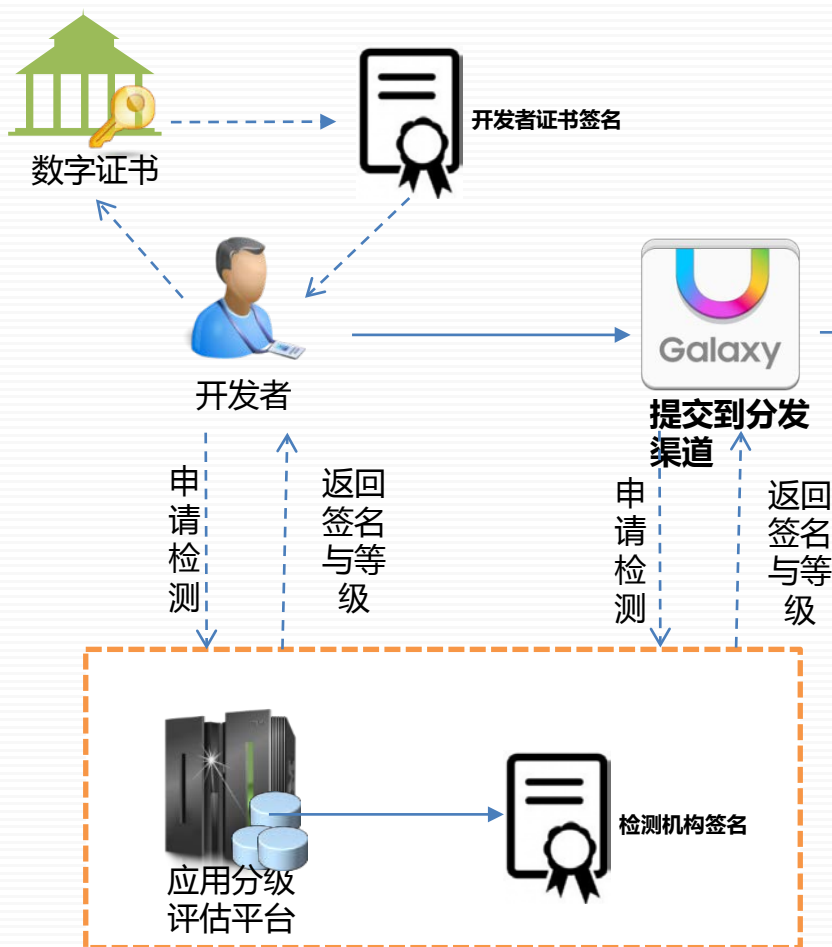




- **恶意、不规范移动应用**是移动智能终端面临的主要安全威胁，已成为阻碍产业进一步健康安全发展的重要因素



基于分级评估与签名管理的移动应用可信生态建设

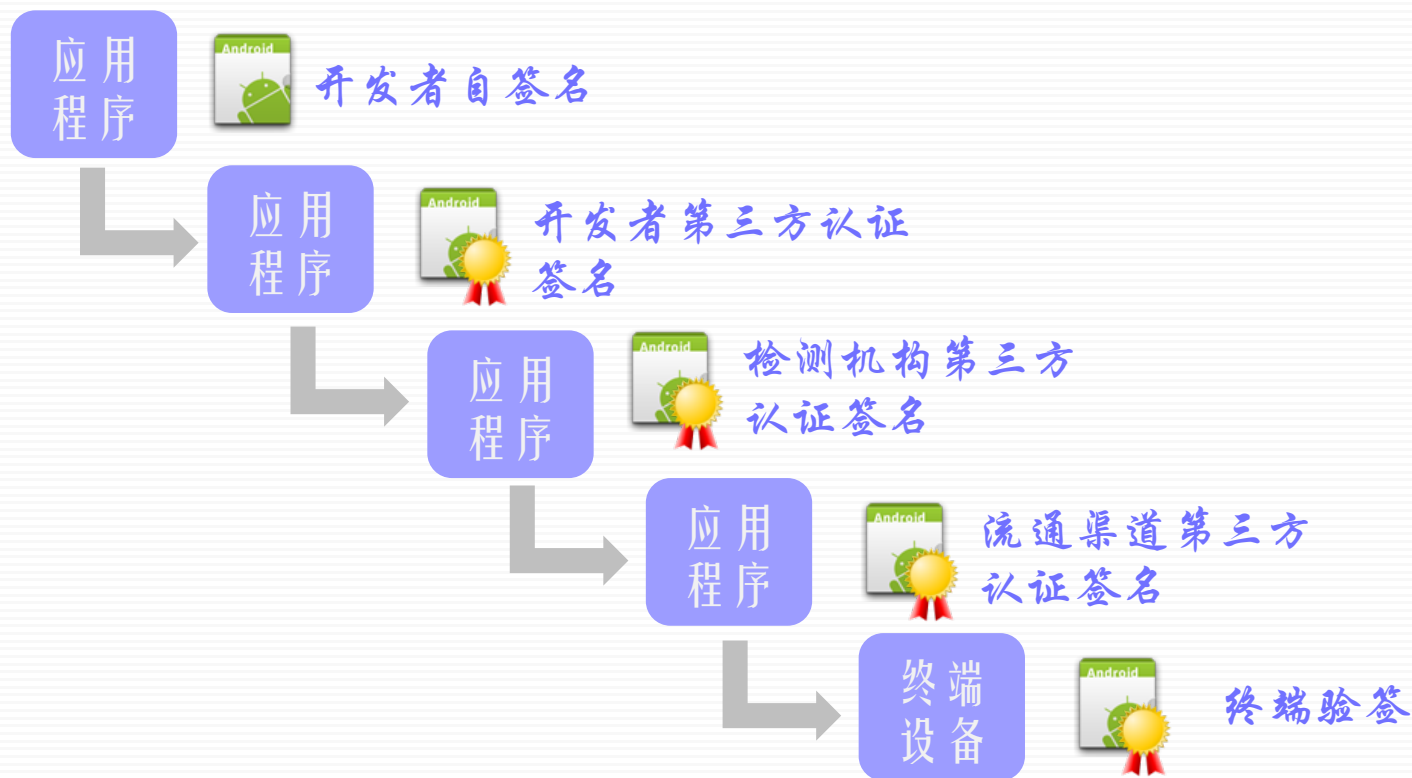


方案核心：

- 1、签名证书：电子认证服务机构颁发的数字证书
- 2、分级评估：《移动应用软件安全评估方法》

工信部《移动智能终端应用软件（APP）预置和分发管理暂行规定》第十条第二款

工业和信息化部鼓励移动智能终端应用软件采用依法设立电子认证服务机构颁发的数字证书进行签名；指导相关企业对已签名的移动智能终端应用软件采用依法设立电子认证服务机构颁发的数字证书，进行验证并显著标识。



政策法规

《全国人大常委会关于维护互联网安全的决定》

国务院《互联网信息服务管理办法》

工信部《移动互联网恶意程序监测与处置机制》

工信部20号令《规范互联网信息服务市场秩序若干规定》

《中华人民共和国广告法(修订)》

工信部《关于加强移动智能终端进网管理的通知》

工信部《移动智能终端应用软件预置与分发管理规定》（待发布）

行业标准

《移动应用软件安全评估方法》

《移动智能终端安全能力技术要求》

《移动终端应用软件安全技术要求》

《移动互联网恶意程序描述格式》

《移动互联网应用商店安全防护要求》

《移动智能终端上的个人信息保护技术要求》

《移动应用广告通用安全技术要求》

标准的背景与目标

恶意应用危害程度不同，缺少细分

应用软件的功能与安全性难以平衡

终端预置应用的备案制度

引导移动应用软件提高自身的安全防护能力。

防范移动应用软件侵犯用户隐私、用户权益，
保证用户的知情权、选择权。

实现对移动应用软件的安全评估



提出与归口	中国通信标准化协会
讨论	TC8 WG2 & TC11 WG2
起草单位	中国信息通信研究院
	中国电信集团公司
	中国联合通信集团公司
	中国移动通信集团公司
	北京奇虎科技有限公司
	深圳市腾讯计算机系统有限公司
	中国科学院软件研究所
可能的用途	工信部移动智能终端进网预置应用测试
	行业协会移动应用软件安全分级评测

应用软件管理

主要针对移动应用软件的安装、卸载、运行、升级行为，对广告、推送等行为，对数据安全、对反编译、反盗版、反注入、看重放有效性进行安全评估。

业务功能调用

主要针对移动应用软件通过各种方式进行拨打电话、三方通话、短信、彩信、邮件、登陆、身份认证、等移动智能终端的业务调用行为进行评估。

外围接口调用

主要针对移动应用软件通过不同方式进行移动通信网络接口、WLAN网络接口、蓝牙接口、NFC接口等移动智能终端外围接口的调用行为进行评估。

用户数据调用

主要针对移动应用软件通过各种方式进行定位功能、通话录音功能、本地录音功能、拍照/摄像功能、短信数据、彩信数据、电话簿信息、通话记录信息、终端系统数据、其他应用数据等移动智能终端中用户数据的调用行为进行评估；

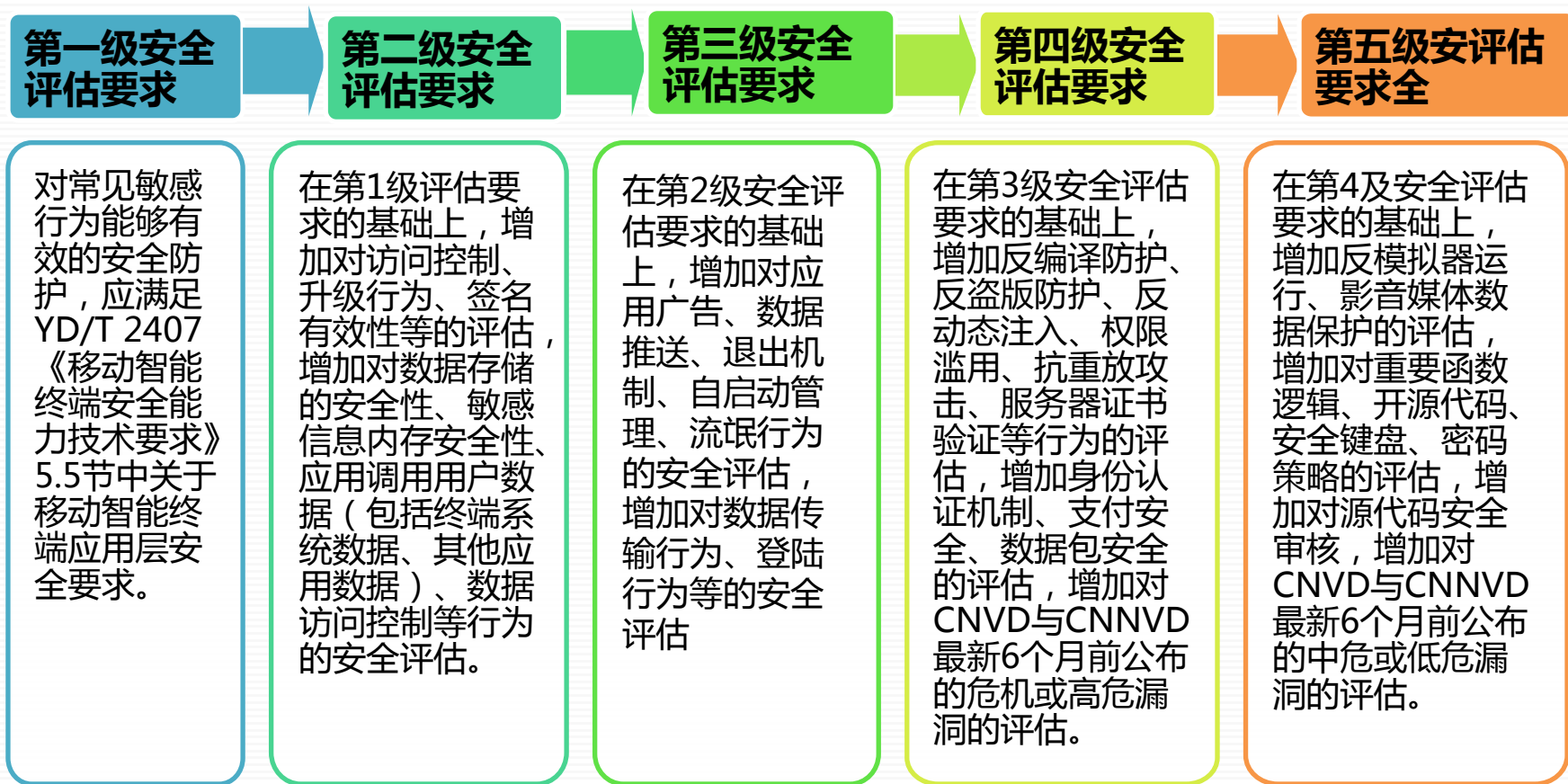
信息内容安全

主要针对移动应用软件使用过程中涉及的文字、图片、影像等内容进行安全评估，保证移动应用软件产生、携带、传输真实信息，不得违反国家法律法规内容。

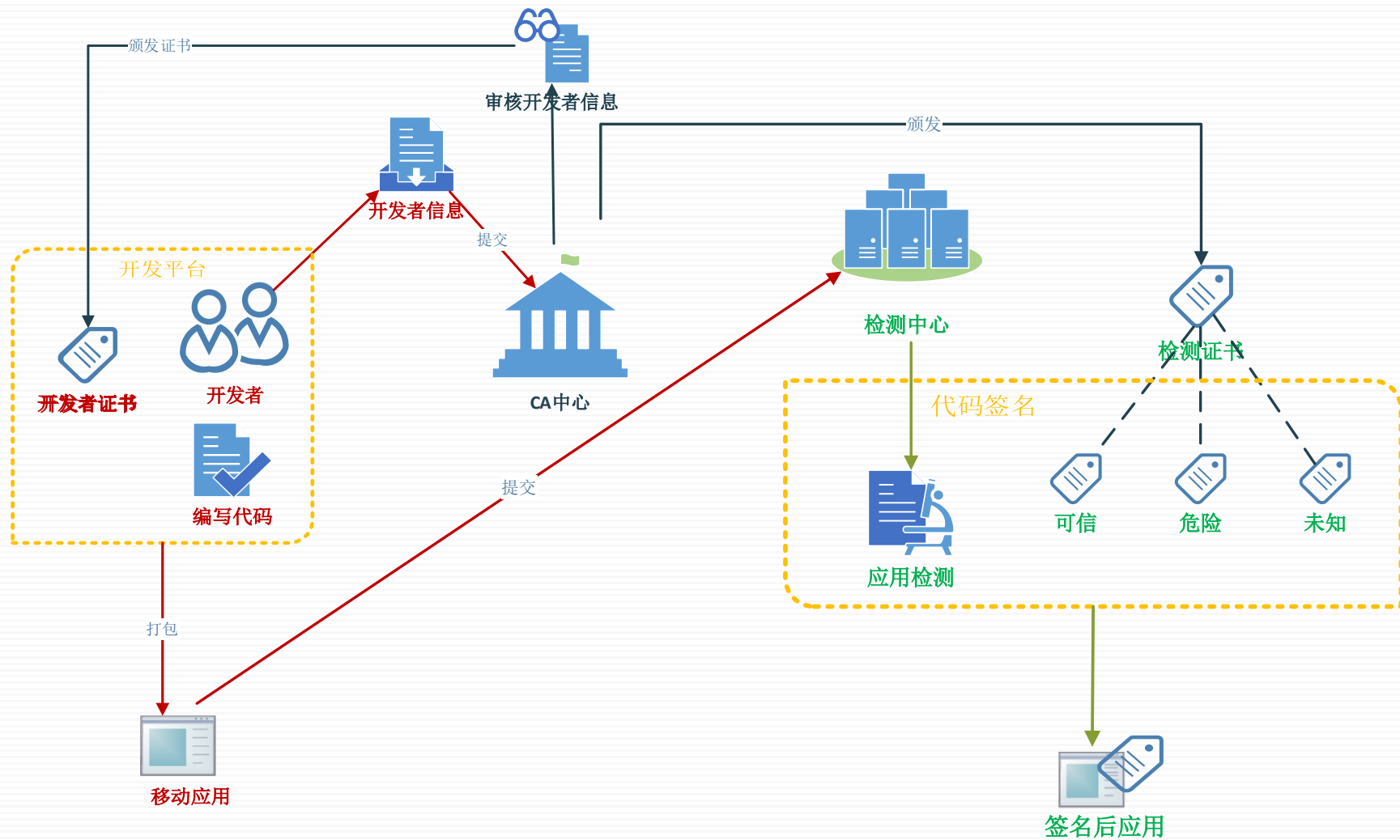
漏洞分析验证

主要针对移动应用软件进行漏洞分析和验证，保证被测移动应用软件中不包含一定时间前CNNVD、CNVD中提交的主要漏洞。

- 依据最小权限、可知可控、安全保障的原则；
- 开发者、终端生产企业、运营商多次讨论；
- 将移动应用安全性划分为五个等级，第五级是最高等级。

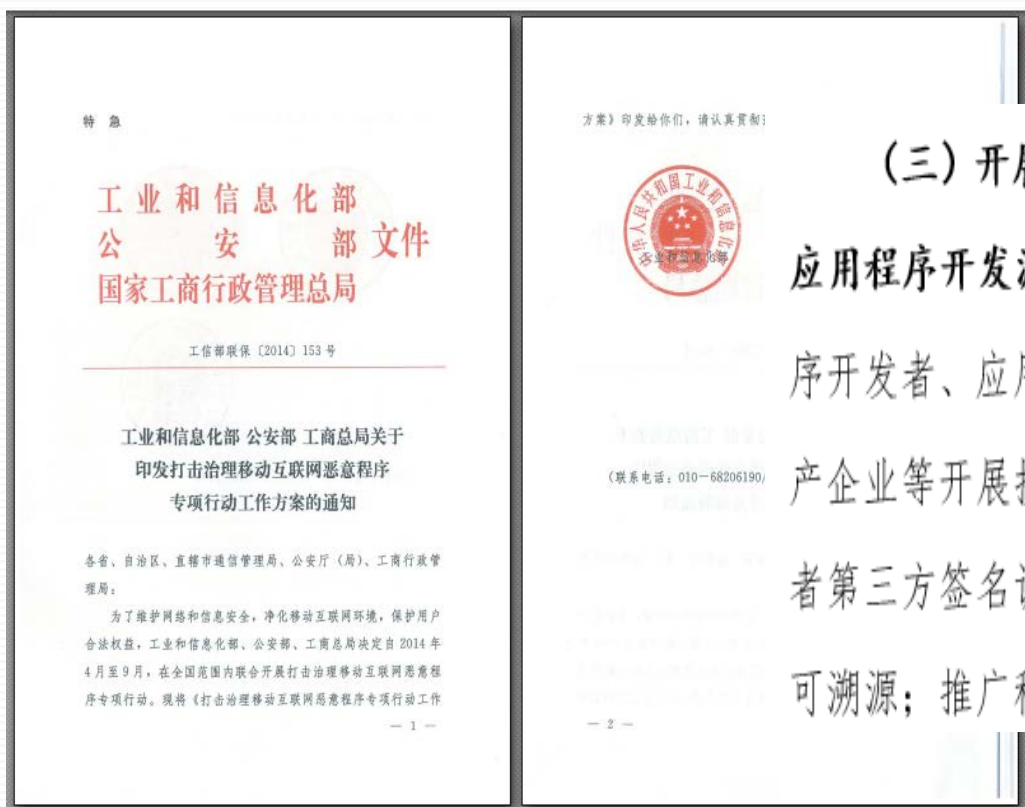


评估签名流程



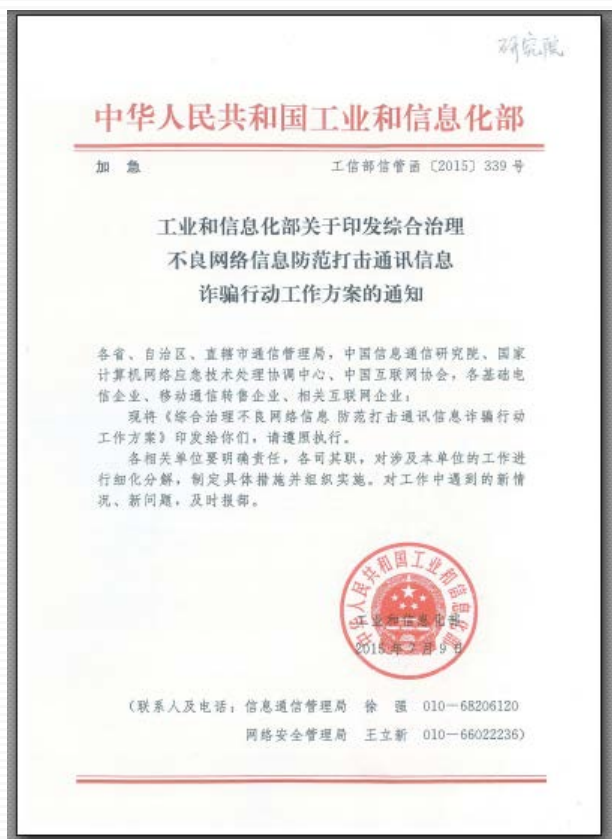


■ 多部委打击治理移动互联网恶意程序专项行动



(三) 开展应用程序开发者第三方签名认证试点, 探索应用程序开发源头管理机制。指导行业协会组织移动应用程序开发者、应用商店、电子认证服务机构、移动智能终端生产企业等开展技术验证和试点工作, 探索建立应用程序开发者第三方签名认证体系的可行性, 实现应用程序的防篡改和可溯源; 推广移动应用程序开发者白名单机制。

■ 综合治理不良网络信息防范打击通讯信息诈骗行动



（二）强化技术手段，提升监测能力

3. 工信部组织建设移动应用程序（APP）安全公共云服务
平台，为终端厂商和消费者自主开展 APP 安全测试提供便利
条件，探索建立 APP 可信认证体系；鼓励用户下载安装安全
防护 APP，推动基础电信企业、相关互联网企业与 12321 举
报中心合作，实现不良网络信息标记数据库信息共享。各通
信管理局组织辖区内基础电信企业，稳妥推进通讯信息诈骗
技术防范手段建设。

■ 移动智能终端应用软件（APP）预置和分发管理暂行规定

附件：

移动智能终端应用软件（APP）预置和分发 管理暂行规定 (征求意见稿)

移动智能终端应用软件(APP)快速发展,为人们的生产、生活带来便利的同时,一些损害用户个人信息和财产安全的问题也逐渐暴露,为保护广大用户合法权益,规范移动互联网市场秩序,维护网络安全,促进信息通信行业健康发展,根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《中华人民共和国电信条例》和《互联网信息服务管理办法》等有关规定,制定本规定。

第一条 为推动移动互联网健康有序发展,构建安全可信的信息通信网络环境,保护广大用户的知情权和选择权,促进大众创业、万众创新,工业和信息化部大力推动移动智能终端应用软件发展,鼓励移动智能终端生产企业、互联网信息服务提供者等相关企业积极开发移动智能终端应用软件产品,丰富信息消费内容,引导企业健全相关管理机制。鼓励有关行业协会依法制定自律性管理制度,共同规范移动智能终端应用软件的预置和分发行为,维护网络安全,加强用户权益保护。

(二)工业和信息化部鼓励移动智能终端应用软件采用依法设立的电子认证服务机构颁发的数字证书进行签名;指导相关企业对已签名的移动智能终端应用软件采用依法设立的电子认证服务机构颁发的数字证书,进行验证并显著标识。

在行业标准协会
内进行应用软件
第三方认证研究

移动互联网应
用软件的安全
认证研究

SR 105-2011
移动数字签名
服务平台研究

推动行业标准协
会进行应用软件
认证标准制定

移动应用程序
代码签名技术
要求

移动应用程序
代码签名测试
方法

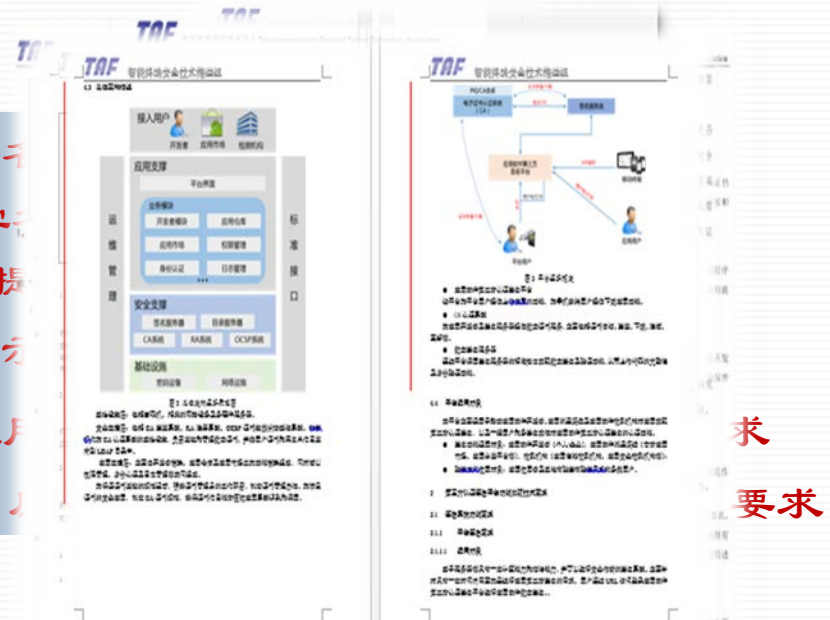


移动应用软件认证实践

■ TAF (电信终端测试认证协会) 开展应用软件第三方认证研究及技术实践

2014年1月14日 应用软件数字签名
2014年4月23日 应用软件数字签名
2014年7月22日 终端验签和提示
2014年12月24日 终端验签和提示
2015年4月2日 (组文件)
2015年7月14日

试点单位



lenovo FOR THOSE WHO DO.



ZTE中兴

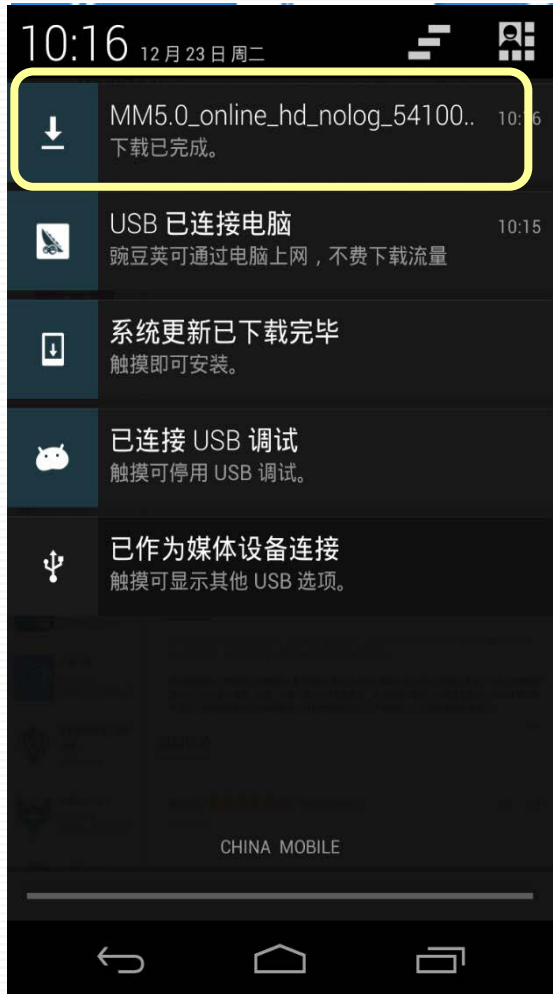
MEDIATEK



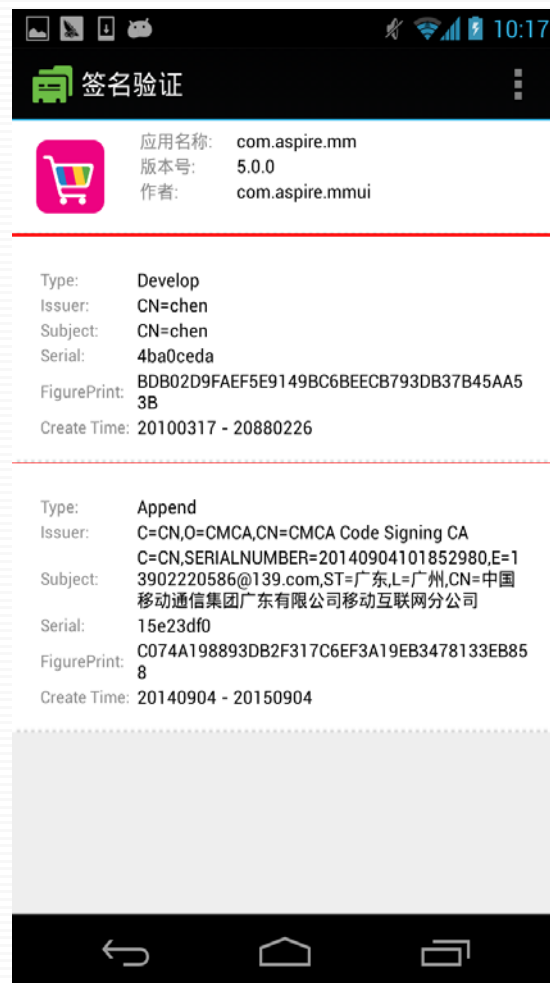
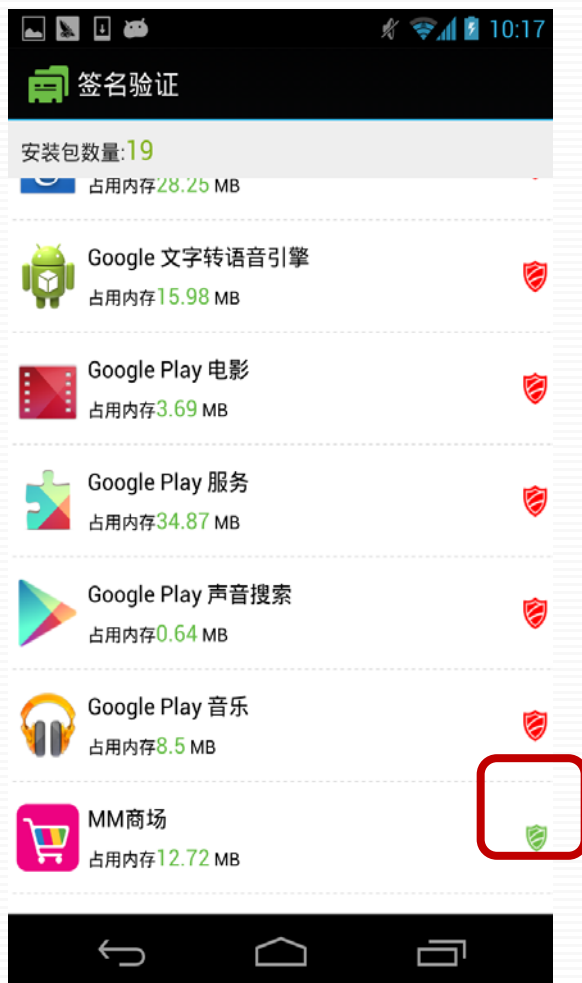
CAICT 中国信息通信研究院
China Academy of Information and Communications Technology

oppo

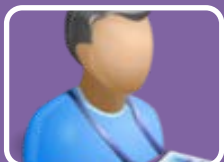
应用软件第三方认证终端验签



应用软件第三方认证终端验签



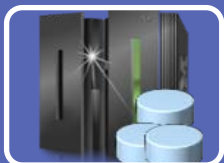




申请开发者证书，提供有效身份信息，获得一定资源



提供移动应用软件、检测机构、流通渠道签名服务，提供终端验签接口



检测机构对应用软件进行五个等级的分级评测，并签名确认



移动应用分发平台提供资源，对优质的、已签名、且做过测试的移动应用进行推广，并签名确认



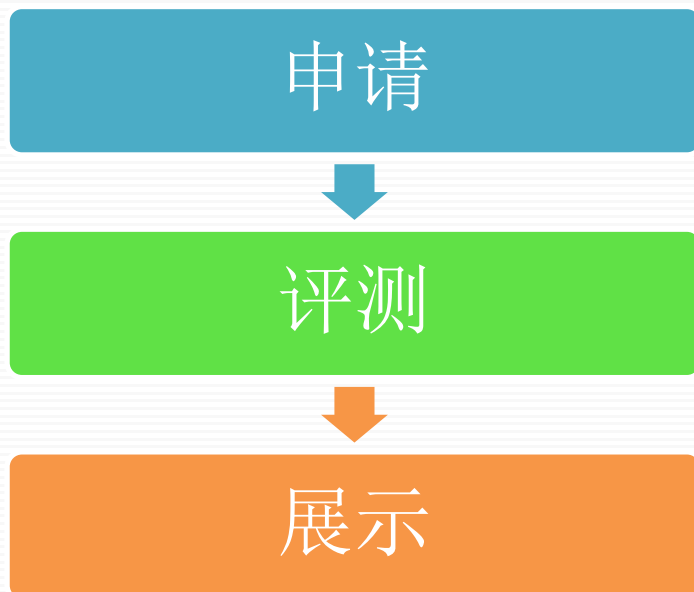
终端侧通过一定方式，向用户展示，实现移动应用软件签名的可视化，管理的可溯源

配合进网安全测试

若操作系统可安装的第三方应用软件均为**单一来源**，且此来源内的应用软件均符合YD/T XXXX—XXXX《移动应用软件安全评估方法》的**三级要求**，则操作系统认为已经具备安全能力。

TAF应用软件分级评测认证

<http://taf.org.cn/Soft.aspx>



谢谢聆听，
敬请批评指正！

