APP安全认证

- 认证流程
- 自评估
    - 自评估内容
    - 自评估材料准备
    - 自评估遇到的问题
- 技术验证
    - 重点检查项
    - 技术验证环节问题
- 现场审核
    - 重点检查项
    - 现场审核环节问题
- 后期维护
    - 何时需要提交自评价报告
    - 证书的变更

> 下文中的《规范》为GB/T 35273《信息安全技术 个人信息安全规范》的简称；
>
> 2019年03月15日 ,市场监管总局及中央网信办发布《关于开展App安全认证工作的公告》。

0 认证流程

整个流程涉及**安全、法务、业务（产品、开发、测试）**的同学共同努力完成。

第一步：提交认证申请及自评估材料，自评估材料主要是针对《规范》5-11的内容；

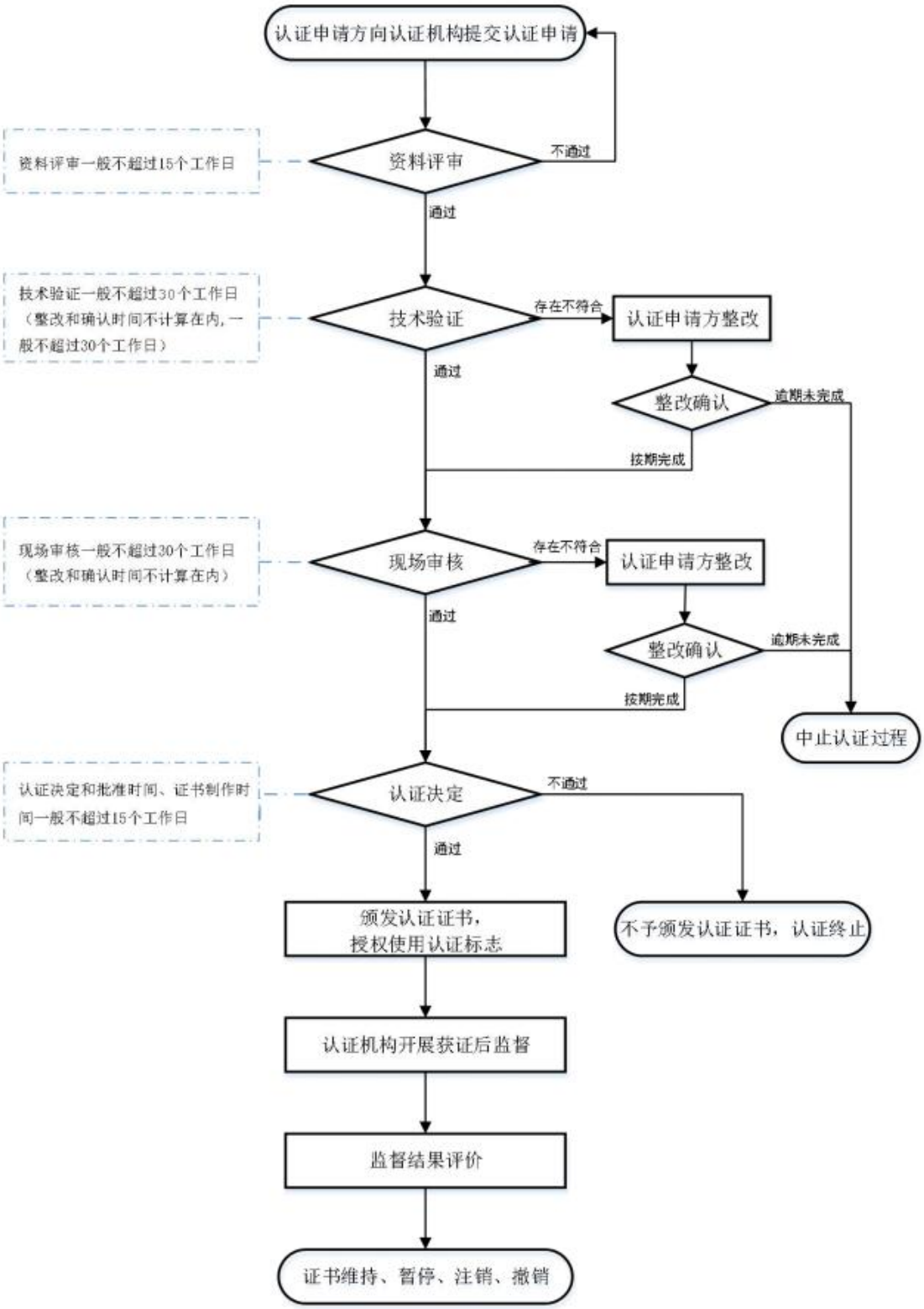
第二步：现场技术认证（主要针对APP及内置功能的是否符合《规范》5-9的内容），根据不合格问题进行整改；

第三步：现场审核（主要针对管理制度是否符合《规范》9-11的内容），根据不合格问题进行整改；

----------到此就可以拿到证书了--------

后续需要进行证书维持，包括版本迭代的信息更新、变化性评估等。

移动互联网应用程序（App）安全认证流程图



1 自评估

《规范》中每一小节进行自评估，将不合规项总结出来进行整改。

1.1 自评估内容

因为公司产品功能比较单一，有些项可能未提及。大致分为：App端测试、后端及运营、隐私政策、内部管理制度四部分。具体检查内容详见下边的脑图（待完善）

1.2 自评估材料准备

申请书附录中的位置并不够展示证明截图，建议使用如下方法准备自评估资料，包括：

编号	5. 1. a
检测要求	不应以欺诈、诱骗、误导的方式收集个人信息
证据截图	
备注	详细说明

1.3 自评估遇到的问题

1. 由于对标准的理解问题，可能会出现多次修改的情况，建议不对外发版，只打测试包就ok。
2. 有些权限/收集信息未触发，可能是无权限进入，或者功能埋点较深，建议多和业务沟通。
3. 不同渠道可能嵌入了不同的SDK，建议逐一测试。

2 技术验证

技术验证主要是针对APP及内置功能的是否符合《规范》5-9的内容进行的，一般测评人员也会进行现场审核。

2.1 重点检查项

- 7.1 个人信息访问控制措施
- 5.5 个人信息保护政策
- 个人信息收集情况（类型、频率、是否明示）
- 注销功能
- 个性化展示
- 第三方SDK使用情况
- 个人信息存储情况

2.2 技术验证环节问题

2.2.1 第三方SDK问题

- 针对第三方接入管理的界定，嵌入第三方SDK是否属于第三方接入，是否需要进行适当接入评估、数据处理协议签订等等。*（开始认为属于-后来不属于-针对目前情况来看还是属于）*

- 第三方SDK应该是数据处理者？数据控制者？数据共享接收方？？？？
    - 如果跳转到第三方平台授权（如使用微信登录、QQ登录等）有品牌露出，这事**独立的数据控制者**。
    - 对于无品牌露出，用户无法感知的SDK应该为**数据数据处理者**，但因目前的形式都是第三方 SDK 提供者与 App 开发者往往通过第三方SDK 提供者的开放平台，在线签署开发者服务协议来约定双方的 权利义务，鲜少有关于委托处理数据方面的专门协议或特别规定，也就难以算作协议双方之间的有效“授权”。无法真正理清责任关系。

2.2.2 个人信息收集/存储的情况

- 在同意隐私政策之前，不应存在敏感个人信息收集的情况
- 敏感信息的收集频率不应过高，对应5.2.b
- 用户输入个人敏感信息的页面，应做提示

2.2.3 其他

- 注销流程要能跑通，符合用户注销相关要求
- 投诉、举报、客服渠道有人响应：如客服电话能接听、QQ申请能同意、人工客服有回复等。
- 个人信息访问控制措施

3 现场审核

3.1 重点检查项

1. 应急预案中是否制定了针对个人信息安全事件的
2. 是否针对开发、设计等人员进行个人信息安全相关的专业化培训及考核，提供记录
3. 安全审计情况
4. 开展个人信息安全影响评估的情况

3.2 现场审核环节问题

3.2.1针对“明确个人信息保护负责人和个人信息保护工作机构”检查项

1. 方法一: 个人信息保护负责人=业务负责人
2. 方法二: 建立信息安全委员会，有机构负责个人信息保护工作。

3.2.2 开展个人信息安全评估

检查存在以下情况时，必须提供个人信息安全评估报告：

1. 存在基于不同业务目的的所收集个人信息的融合汇聚
2. 存在信息系统自动决策机制
3. 存在委托处理、数据共享、个人信息公开披露情况

4 后期维护

4.1 何时需要提交自评价报告

(1)获证App的分发渠道发生变化;

(2)认证标志使用情况发生变化;

(3)获证App隐私政策发生变化;

(4)获证App收集、处理和使用个人信息的目的、类型、方式发生变化;

(5)获证App运营者对所收集个人信息的共享、转让、公开披露的对象、方式和目的发生变化;

(6)获证App运营者收到获证App个人信息保护相关的投诉举报。

4.2 证书变更

出现下列情况之一时，获证App运营者应向认证机构提出变更申请:

(1)获证App名称、版本发生变更;

(2)认证范围扩大或缩小;

(3)获证App运营者名称、注册地址发生变更;

注：大版本变更、小版本新增功能新增涉及个人信息收集等情况会涉及变更费用、技术验证、现场审核费用。

渠道方收集内容：

1. 渠道SDK收集的个人信息
2. 发送给渠道网站的

获取权限

1. 渠道sdK获取的权限
2. 待定：多余官方的权限

权限获取方式

1. 登陆即获取权限
2. 触发式获取
3. 是否可关闭

App和SDK

“当第三方 SDK 可以直接透过 App 露出自己品牌时，App 开发者更 容易让 SDK 提供方独自成为个人信息的数据控制者”，例如：微信登录SDK、微博登录SDK等

当第三方 SDK 可以直接透过 App 露出自己品牌时，App 开发者更 容易让 SDK 提供方独自成为个人信息的数据控制者，故，应当在 App 《隐私政策》的共享章节或者展示 SDK 的专门章节介绍 App 接入了哪 些具体的第三方 SDK、向这些第三方 SDK 共享个人信息的目的、功能、 范围、开启权限等情况、第三方 SDK 的隐私政策情况（如有）；如果 在披露第三方 SDK 的隐私政策时，可实现跳转至第三方 SDK 官方服务 页面的，建议向用户直接展示该第三方 SDK 的《隐私政策》。此时需 要注意的是，披露的颗

粒度建议具体到每个实际提供服务的 SDK。