# Android端隐私合规检测技术方案

## 方案技术背景

隐私合规检测整体基于（MobSF）开源移动应用自动测试框架原理。该平台可对安卓、苹果应用程序进行静态、动态分析，并在web端输出报告。静态分析适用于安卓、苹果应用程序。

## **静态检测**

静态分析主要包含三个部分，分别是Manifest Analysis、Cert Analysis、Code Analysis。流程如下:



1. **Manifest Analysis分析**

解压apk后，使用AXMLPrinter2.jar工具提取app中的AndroidManifest.xml文件内容，并进行分析。ManifestAnalysis主要功能是对AndroidManifest.xml进行解析，提取其中permission、granturipermissions、application、activties、services、intents、actions等，分析所有权限并对权限进行分级，包含正常、危险、签名、系统四个类别。对各属性配置进行检查，看是否存在不安全的配置，如allowBackup、debuggable、exported等属性设置。

1. **Cert Analysis分析**

MobSF证书分析功能函数在cert\_analysis.py文件中，MobSF首先尝试获取Hardcoded Certificates/Keystores，然后通过CertPrint.jar工具解析apk中证书的信息，并完成证书相关问题的分析。

1. **Code Analysis分析**

MobSF静态代码分析功能函数在code\_analysis.py文件中，反编译的代码在converter.py中。其中使用Dex2Jar将dex转变为jar文件，使用Dex2Smali将dex转变为smali代码，使用jd-core.jar、cfr\_0\_115.jar、procyon-decompiler-0.5.30.jar将jar包转为为可读的java代码。

最后利用正则表达式对反编译得到的java源码进行匹配来实现的。主要通过匹配常见方法中的关键词来提取源码中用到的方法。以及匹配敏感关键词来提取账号密码等信息。