Evaluation Warning: The document was created with Spire.Doc for Python.

**民政部（ 1.0.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 民政部 |
| 版本 | 1.0.0 |
| 包名 | com.klmsqq.kbgxhyg |
| 域名线索 | 29条 |
| URL线索 | 27条 |
| APP图标 |  |
| 分析日期 | 2025年6月17日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 民政部.apk |
| 文件大小 | 6.76MB |
| MD5值 | c54071d7728ad6a65e5b751fec3042ca |
| SHA1值 | 8390adcb07f61a07f4031387490060cb8bf2def5 |
| SHA256值 | 6bd3e7b18b210e631a3499f8fe06c52f0b5126bc5320155fa7c5b4c4fb6e799b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 民政部 |
| 包名 | com.klmsqq.kbgxhyg |
| 主活动Activity | com.bslyun.app.activity.MainActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 4 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| testdatalbs.sparta.html5.qq.com | IP: 157.255.4.30 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| nlp.map.qq.com | IP: 116.130.220.122 所属国家: China 地区: Beijing 城市: Beijing  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| my.wlwx.com | IP: 120.24.95.120 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| maps.google.com | IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto  |
| wx.tenpay.com | IP: 210.22.240.151 所属国家: China 地区: Shanghai 城市: Shanghai  |
| adblocker.appbsl.net | 没有服务器地理信息.  |
| api.weibo.com | IP: 116.133.8.18 所属国家: China 地区: Beijing 城市: Beijing  |
| www.appk6.com | IP: 156.224.140.92 所属国家: United States of America 地区: California 城市: San Jose  |
| api.appbsl.net | IP: 61.48.83.207 所属国家: China 地区: Beijing 城市: Beijing  |
| auth.appbsl.com | 没有服务器地理信息.  |
| pms.mb.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cc.map.qq.com | IP: 125.36.181.145 所属国家: China 地区: Tianjin 城市: Tianjin  |
| lstest.map.qq.com | IP: 116.130.223.83 所属国家: China 地区: Beijing 城市: Beijing  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cs.map.qq.com | IP: 125.36.181.143 所属国家: China 地区: Tianjin 城市: Tianjin  |
| schemas.android.com | 没有服务器地理信息.  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| analytics.map.qq.com | IP: 125.36.181.142 所属国家: China 地区: Tianjin 城市: Tianjin  |
| rttgpsreport.map.qq.com | IP: 60.28.215.105 所属国家: China 地区: Tianjin 城市: Tianjin  |
| com.thoughtworks.xstream | 没有服务器地理信息.  |
| ue.indoorloc.map.qq.com | IP: 116.130.224.171 所属国家: China 地区: Beijing 城市: Beijing  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| work.weixin.qq.com | IP: 106.55.209.39 所属国家: China 地区: Beijing 城市: Beijing  |
| tbs.imtt.qq.com | IP: 36.248.43.86 所属国家: China 地区: Fujian 城市: Fuzhou  |
| ns.adobe.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://ns.adobe.com/xap/1.0/\u0000  | a/e/a/a.java  |
| https://lstest.map.qq.com/nlpdr?sf  | c/t/m/g/j.java  |
| https://nlp.map.qq.com/?sf  | c/t/m/g/j.java  |
| https://testdatalbs.sparta.html5.qq.com/tr?sf  | c/t/m/g/j.java  |
| https://analytics.map.qq.com/?sf  | c/t/m/g/j.java  |
| https://cs.map.qq.com/atta?type=1&multi=0  | c/t/m/g/s3.java  |
| https://analytics.map.qq.com/tr?mllc  | c/t/m/g/s3.java  |
| https://cs.map.qq.com/key  | c/t/m/g/r0.java  |
| https://analytics.map.qq.com/tr?mllc  | c/t/m/g/r6.java  |
| https://rttgpsreport.map.qq.com/report?type=sdk&key=5e1fe70424035ee83066ac22b24f31dc  | c/t/m/g/f.java  |
| https://cc.map.qq.com/?get\_c3  | c/t/m/g/m0.java  |
| https://ue.indoorloc.map.qq.com/?wl  | c/t/m/g/u4.java  |
| https://testdatalbs.sparta.html5.qq.com/tr?wf4  | c/t/m/g/h.java  |
| https://analytics.map.qq.com/?wf4  | c/t/m/g/h.java  |
| https://testdatalbs.sparta.html5.qq.com/tr?utr  | c/t/m/g/g.java  |
| https://analytics.map.qq.com/tr?utr  | c/t/m/g/g.java  |
| https://apis.map.qq.com/ws/geocoder/v1/?location=  | c/t/m/g/p4.java  |
| http://www.appk6.com  | com/bslyun/app/MainApplication.java  |
| https://wx.tenpay.com/  | com/bslyun/app/browser/WebViewUtils.java  |
| http://maps.google.com/maps?saddr=  | com/bslyun/app/browser/Bridge.java  |
| https://work.weixin.qq.com/kfid/  | com/bslyun/app/browser/Bridge.java  |
| https://api.weibo.com/2/users/  | com/bslyun/app/component/WeiboComponent.java  |
| https://my.wlwx.com:6016  | com/bslyun/app/component/quicklogin/QuickLoginComponent.java  |
| http://auth.appbsl.com  | com/bslyun/app/component/quicklogin/QuickLoginComponent.java  |
| https://wx.tenpay.com/  | com/bslyun/app/fragment/WebFragment.java  |
| http://api.appbsl.net/adv/index/appcount?mark=7&type=100  | com/bslyun/app/e/a.java  |
| https://adblocker.appbsl.net/index.php?g=port&m=unionadvblock&a=get  | com/bslyun/app/service/UpdateFilterIpService.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/k.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/o.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/o.java  |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs  | com/tencent/smtt/utils/d.java  |
| http://com.thoughtworks.xstream/sax/property/configured-xstream  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/sax/property/source-object-list  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://xml.org/sax/features/namespaces  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/sax/property/configured-xstream\  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/sax/property/source-object-list\  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/XStreamSource/feature  | com/thoughtworks/xstream/io/xml/TraxSource.java  |
| http://schemas.android.com/apk/res/android  | com/xuexiang/xui/widget/banner/widget/banner/base/BaseBanner.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| x5tbs@tencent.com  | com/tencent/smtt/sdk/X5Downloader.java  |
| null@null.xml  | com/thoughtworks/xstream/persistence/FilePersistenceStrategy.java  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, O=���������, OU=���������, CN=403259 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-11 16:56:50+00:00 有效期至: 2123-12-04 16:56:50+00:00 发行人: C=CN, O=���������, OU=���������, CN=403259 序列号: 0x581bcfd0 哈希算法: sha256 md5值: e3dba029d4ad98ab7ad89dfef7a07009 sha1值: fd047db1bf7c7c48ee8c6ca0197caf633c50e78c sha256值: daadf67b90871419bc2fbf44f3e95884b4a63a053a7613e2d13728e6ba587872 sha512值: 17f813784523d4a5e4c3ee80f3694d07f7b15ce0a3ec79104faa8797ad7d81a4f69570f340c1b6c151b174b4fe0af60aa7c7cfe553614853c7888a00ea42a780 公钥算法: rsa 密钥长度: 2048 指纹: 1141c4149ef61da9a709c4d23570f04a862a75bc5f494d9f4f577df1610533b0**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "QQ\_AppSecret" : "\_QQ\_AppSecret"  |
| "SINA\_APP\_KEY" : "\_SINA\_APP\_KEY"  |
| "WX\_AppSecret" : "\_WX\_AppSecret"  |
| "adset\_app\_key" : ""  |
| "ali\_login\_secret\_key" : ""  |
| "baid\_ai\_app\_key" : "\_baid\_ai\_app\_key"  |
| "baid\_ai\_secret\_key" : "\_baid\_ai\_secret\_key"  |
| "baidu\_face\_api\_key" : ""  |
| "baidu\_face\_secret\_key" : ""  |
| "hw\_app\_key" : "\_hw\_app\_key"  |
| "lebo\_app\_secret" : "\_lebo\_app\_secret"  |
| "linked\_me\_key" : ""  |
| "meiqia\_app\_key" : ""  |
| "mi\_app\_key" : "\_mi\_app\_key"  |
| "my\_app\_secret" : ""  |
| "my\_master\_secret" : ""  |
| "oppo\_app\_key" : ""  |
| "rongyun\_appkey" : ""  |
| "tx\_tts\_secret\_id" : ""  |
| "tx\_tts\_secret\_key" : ""  |
| "umeng\_app\_key" : ""  |
| "zb\_license\_key" : ""  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CLEAR\_APP\_CACHE | 系统需要 | 删除所有应用程序缓存数据 | 允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。  |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ASSISTED\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| com.fingerprints.service.ACCESS\_FINGERPRINT\_MANAGER | 未知 | Unknown permission | Unknown permission from android reference |
| com.samsung.android.providers.context.permission.WRITE\_USE\_APP\_FEATURE\_SURVEY | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.bslyun.app.activity.MainActivity | **Schemes**: @string/wx\_app\_id://, @string/u\_link\_scheme://, um.622017db317aa87760767d8c://, mtjç¦\u0081æ­¢å\u0088 é\u0099¤://,  |
| com.bslyun.app.activity.HtmlOpenApp | **Schemes**: bslapp://,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**