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

**兔獴身份验证器Authenticator（ 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 | 兔獴身份验证器Authenticator |
| 版本 | 1.0.0 |
| 包名 | com.kehui.tumengverify |
| 域名线索 | 11条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | tumeng.apk |
| 文件大小 | 11.25MB |
| MD5值 | 5a43865afcfbb97520f4701fae8253f6 |
| SHA1值 | 030296041bbcb916ad1f25589dcc11379bac94b7 |
| SHA256值 | 7c3157927f212e2855c660e9c98b2e0645778fa3eaa521f2b9043ca09f805d94 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 兔獴身份验证器Authenticator |
| 包名 | com.kehui.tumengverify |
| 主活动Activity | com.kehui.tumengverify.HomeActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.aaaaaaaa.com | IP: 64.190.63.222 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Koeln  |
| ip.taobao.com | IP: 59.82.122.140 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| t.me | IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington  |
| ip.chinaz.com | IP: 123.129.219.142 所属国家: China 地区: Shandong 城市: Jinan  |
| tmaut.com | IP: 172.67.147.162 所属国家: United States of America 地区: California 城市: San Francisco  |
| pv.sohu.com | IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing  |
| auth.xinwuka.com | IP: 139.129.235.158 所属国家: China 地区: Shandong 城市: Qingdao  |
| www.foxupay.com | IP: 104.21.31.160 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| schemas.android.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/PermissionUtils.java  |
| https://www.foxupay.com/agreement/energy.html  | com/kehui/tumengverify/utils/Const.java  |
| http://pv.sohu.com/cityjson  | com/kehui/tumengverify/utils/MacgetUtils.java  |
| http://pv.sohu.com/cityjson?ie=utf-8  | com/kehui/tumengverify/utils/MacgetUtils.java  |
| http://ip.taobao.com/service/getIpInfo2.php?ip=myip  | com/kehui/tumengverify/utils/MacgetUtils.java  |
| http://ip.chinaz.com/getip.aspx  | com/kehui/tumengverify/utils/MacgetUtils.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | org/java\_websocket/AbstractWebSocket.java  |
| http://api.aaaaaaaa.com/web/  | 摸瓜V1引擎  |
| https://t.me/+Ry8pEQ1RIKczNjkx  | 摸瓜V1引擎  |
| https://t.me/FOXUPAY  | 摸瓜V1引擎  |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1引擎  |
| https://tmaut.com/api  | 摸瓜V1引擎  |
| http://auth.xinwuka.com/api  | 摸瓜V1引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| user@example.com admin@foxupay.com  | 摸瓜V1引擎  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=kehui OU=kehui 签名算法: rsassa\_pkcs1v15 有效期自: 2024-11-11 03:55:01+00:00 有效期至: 2034-11-09 03:55:01+00:00 发行人: CN=kehui OU=kehui 序列号: 0x4881483a 哈希算法: sha256 md5值: d7aa8d0e20bb5a88a13e3779bc93b9a6 sha1值: 0e61d496e7e129f55ccb913812a7dbf7c475759f sha256值: e379a87cbed740276584d4afe2bcaa11955ae8d76d983a3629c3d6af22eeb9fa sha512值: f799400ad66af6f79a8b2b258fbf8349c8b556388ad8a95b3797508e3b279b2372cf8b4080e170ab14068e0cd5e0c87bf8dff9e0606d03068c4c547a44d62e7c 公钥算法: rsa 密钥长度: 2048 指纹: 5003ae4103858b471b8ae53d3db79e78ad3581294543d6ecb109f5b5cd358807**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "apikey" : "API秘钥"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "nosecretkey" : "暂无添加秘钥"  |
| "pleaseinputsecretkey" : "请输入秘钥"  |
| "secretkey" : "秘钥"  |
| "setpassword" : "设置密码"  |
| "apikey" : "API秘鑰"  |
| "setpassword" : "設置密碼"  |
| "apikey" : "API key"  |
| "setpassword" : "Set password"  |
| "apikey" : "API秘鑰"  |
| "setpassword" : "設置密碼"  |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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\_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.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.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 |
| android.permission.USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| com.kehui.tumengverify.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**