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

**Authenticator（ 1.1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 | Authenticator |
| 版本 | 1.1 |
| 包名 | com.authenticator |
| 域名线索 | 18条 |
| URL线索 | 17条 |
| APP图标 |  |
| 分析日期 | 2025年7月18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 | 2\_base.apk |
| 文件大小 | 47.97MB |
| MD5值 | 4c317d6c9dbbd769a7ecaa87cd04d6c1 |
| SHA1值 | 7737372d5dacb478f83e32d66f3234c2c2bafe52 |
| SHA256值 | 69ed2aa000ab9ad174d41335a0e9f751cc72a80e9b2e53ce1aae669ec18d2568 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Authenticator |
| 包名 | com.authenticator |
| 主活动Activity | com.authenticator.SplashActivity |
| 安卓版本名称 | 1.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| iptc.org | IP: 3.64.29.21 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| cipa.jp | IP: 118.82.81.189 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| xerces.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| www.npes.org | IP: 104.21.43.185 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| ns.useplus.org | IP: 54.83.4.77 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| raw.githubusercontent.com | IP: 185.199.110.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| connectivitycheck.gstatic.com | IP: 203.208.49.66 所属国家: China 地区: Beijing 城市: Beijing  |
| javax.xml.xmlconstants | 没有服务器地理信息.  |
| drewnoakes.com | IP: 34.229.76.186 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| android.googlesource.com | IP: 74.125.20.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.aiim.org | IP: 199.60.103.225 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| purl.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://ns.adobe.com/StockPhoto/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/asf/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/bwf/bext/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/camera-raw-settings/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/creatorAtom/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/xmp/XMPConst.java  |
| http://purl.org/dc/1.1/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/DICOM/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/1.0/DynamicMedia/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://cipa.jp/exif/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/adobe/xmp/XMPConst.java  |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/  | com/adobe/xmp/XMPConst.java  |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/iX/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/jp2k/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/jpeg/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/pdf/1.3/  | com/adobe/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/extension/  | com/adobe/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/field  | com/adobe/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/id/  | com/adobe/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/property  | com/adobe/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/schema  | com/adobe/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/type  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/pdfx/1.3/  | com/adobe/xmp/XMPConst.java  |
| http://www.npes.org/pdfx/ns/id/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/photoshop/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.useplus.org/ldf/xmp/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/png/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/album/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/riff/info/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/1.0/Script/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/swf/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/tiff/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/transient/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/TransformXMP/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/wav/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/bj/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/mm/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/note/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/rights/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Dimensions  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Font  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/g/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/Identifier/qual/1.0/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/g/img/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/ManifestItem  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/t/pg/  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/ResourceEvent  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/ResourceRef  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Job  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Version  | com/adobe/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/t/  | com/adobe/xmp/XMPConst.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/xmp/impl/Utils.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/xmp/impl/Utils.java  |
| http://ns.adobe.com/tiff/1.0/  | com/adobe/xmp/impl/Utils.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/xmp/impl/Utils.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/adobe/xmp/impl/Utils.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/tiff/1.0/  | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/xmp/impl/XMPSerializerRDF.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/xmp/impl/ParseRDF.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/xmp/impl/XMPNormalizer.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/xmp/impl/XMPNormalizer.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | com/adobe/xmp/impl/XMPMetaParser.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | com/adobe/xmp/impl/XMPMetaParser.java  |
| http://xml.org/sax/features/external-general-entities  | com/adobe/xmp/impl/XMPMetaParser.java  |
| http://xerces.apache.org/xerces2-j/features.html  | com/adobe/xmp/impl/XMPMetaParser.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/adobe/xmp/impl/XMPMetaParser.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | com/adobe/xmp/impl/XMPMetaParser.java  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s\  | com/drew/imaging/ImageMetadataReader.java  |
| http://purl.org/dc/elements/1.1/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/exif/1.0/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/tiff/1.0/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/xap/1.0/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/xmp/note/  | com/drew/metadata/xmp/XmpReader.java  |
| http://ns.adobe.com/xmp/extension/\u0000  | com/drew/metadata/xmp/XmpReader.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | com/drew/metadata/xmp/XmpReader.java  |
| https://drewnoakes.com/code/exif/\n  | com/drew/tools/ProcessAllImagesInFolderUtility.java  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/%s)  | com/drew/tools/ProcessAllImagesInFolderUtility.java  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/metadata/%s.txt)\n  | com/drew/tools/ProcessAllImagesInFolderUtility.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenStackFragment.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | 摸瓜V3引擎  |
| play.googleapis.com  | 摸瓜V3引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.html/var/run/egd-pool/dev/egd-pool/etc/egd-pool/etc/entropy/dev/u  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/clang  | 摸瓜V3引擎  |
| connectivitycheck.gstatic.com  | 摸瓜V3引擎  |
| http://www.aiim.org/pdfa/ns/property#  | 摸瓜V3引擎  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/metadata/%s.txt  | 摸瓜V3引擎  |
| http://xerces.apache.org/xerces2-j/features.html#external-parameter-entities  | 摸瓜V3引擎  |
| http://%s/%s.%s?platform=android&dev=%s&minify=%s&app=%s&modulesOnly=%s&runModule=%s%s  | 摸瓜V3引擎  |
| http://www.aiim.org/pdfa/ns/type#  | 摸瓜V3引擎  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s  | 摸瓜V3引擎  |
| http://ns.useplus.org/ldf/xmp/1.0/  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm  | 摸瓜V3引擎  |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/  | 摸瓜V3引擎  |
| http://xml.org/sax/features/external-parameter-entities  | 摸瓜V3引擎  |
| https://drewnoakes.com/code/exif/  | 摸瓜V3引擎  |
| http://apache.org/xml/features/disallow-doctype-decl  | 摸瓜V3引擎  |
| clientservices.googleapis.com  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/%s  | 摸瓜V3引擎  |
| http://xml.org/sax/features/external-general-entities  | 摸瓜V3引擎  |
| gmscompliance-pa.googleapis.com  | 摸瓜V3引擎  |
| http://www.npes.org/pdfx/ns/id/  | 摸瓜V3引擎  |
| http://www.aiim.org/pdfa/ns/field#  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://www.aiim.org/pdfa/ns/schema#  | 摸瓜V3引擎  |
| http://cipa.jp/exif/1.0/  | 摸瓜V3引擎  |
| https://github.com/facebook/react-native/wiki/Breaking-Changes#d4611211-reactnativeandroidbreaking-m  | 摸瓜V3引擎  |
| http://www.aiim.org/pdfa/ns/id/  | 摸瓜V3引擎  |
| http://xerces.apache.org/xerces2-j/features.html#disallow-doctype-decl  | 摸瓜V3引擎  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.html  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067  | 摸瓜V3引擎  |
| http://www.android.com/  | 摸瓜V3引擎  |
| http://www.aiim.org/pdfa/ns/extension/  | 摸瓜V3引擎  |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.html  | lib/x86/libconceal.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libnative-imagetranscoder.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libconceal.so  |

### **4.3 邮箱线索**

### **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=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug 签名算法: rsassa\_pkcs1v15 有效期自: 2013-12-31 22:35:04+00:00 有效期至: 2052-04-30 22:35:04+00:00 发行人: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug 序列号: 0x232eae62 哈希算法: sha1 md5值: 20f46148b72d8e5e5ca23d37a4f41490 sha1值: 5e8f16062ea3cd2c4a0d547876baa6f38cabf625 sha256值: fac61745dc0903786fb9ede62a962b399f7348f0bb6f899b8332667591033b9c sha512值: 926c0550edaee7aed1211b91fde06be4cc4748e61d8f1afbe0bd12f3949a0d09a1cf4306c72e6662ae4c7b8ae7a573a81d7e52e5b6124444eaf8f413e6b1fa69 公钥算法: rsa 密钥长度: 2048 指纹: b759a55bdc298b16f7a102f3107f3db38110f3dc7da00b1e981e9b257a9cf1af**

## **6. 硬编码敏感信息**

## **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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| 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.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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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 |

## **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。**