南明离火
移动应用检测平台

ANDROID 静态分析报告

Authenticate • v25.1.22

分析日期: 2025-03-11 10:02:16

应用概览

文件名称:	Authenticate v25.1.22.apk
文件大小:	20.06MB
应用名称:	Authenticate
软件包名:	secureauth.android.token
主活动:	com.accepttomobile.common.ui.splash.SplashActivity
版本号:	25.1.22
最小SDK:	23
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	48/100 (中风险)
跟踪器检测:	4/432
杀软检测:	2 个杀毒软件报毒
MD5:	d52002438b7bc04e9db44485176026bc
SHA1:	12f2d7b2a074e45c723c15c7d15f1a89fcd18880
SHA256:	f2962a4849b9b4a26c4e521eb894f03f38cffe095e90eb5f1279d62f5864aa1

分析结果严重性

高危	中危	信息	安全	关注
5	27	4	3	2

四大组件信息

Activity组件：41个，其中export的有： 1个
Service组件：21个，其中export的有： 3个
Receiver组件：16个，其中export的有： 4个
Provider组件：4个，其中export的有： 0个

证书信息

二进制文件已签名

v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=CA, L=Irvine, O=SecureAuth Corp, OU=Software, CN=SecureAuth
签名算法: rsassa_pkcs1v15
有效期自: 2013-03-28 21:05:42+00:00
有效期至: 2043-03-21 21:05:42+00:00
发行人: C=US, ST=CA, L=Irvine, O=SecureAuth Corp, OU=Software, CN=SecureAuth
序列号: 0x5154b0a6
哈希算法: sha1
证书MD5: 58fadbb3fe4d20d0fd1701e89ffd1056
证书SHA1: f29263d08f8a749d11039c5ff95a4ec8ce242efe
证书SHA256: 4c8c18a7269c02df90da7b1d85326bf0073a5ab0a5e3511f4f74a3f315cdcd75
证书SHA512:
de662479c04e4007848c6ec2c7de69abb1f2c1b49a0fa064de71d09ed437e0c82231aadb88772e00f0b961b003b3d449ba10cb2c3e0acdd4118bd247532a49df

公钥算法: rsa
密钥长度: 1024
指纹: fea430f4fc85d128994604c2820da4117c3fac750009d0e3dcff7c9cfdd6f2c4
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	未知权限	来自 android 引用的未知权限。
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_WIFI_STATE	普通	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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。

android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
com.acceptto.m2m.permission.UA_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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SD卡内容	允许应用程序从SD卡读取信息。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
android.permission.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
secureauth.android.token.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	未知权限	来自 android 引用的未知权限。
android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
org.fidoalliance.uaf.permissions.FIDO_CLIENT	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.fido.uaf.asm.permissions.FIDO_UAF_ASM	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT

com.acceptomobile.common.ui.start.StartActivity	Schemes: https://, mfa.acceptto.com://, dev.eguardian.io://, m2m.acceptto.net://, eg.coupang.acceptto.com://, secureauthotp://, Hosts: mfa.acceptto.com, dev.eguardian.io, m2m.acceptto.net, eg.coupang.acceptto.com, app, Path Prefixes: /app,

网络通信安全

高危: **1** | 警告: **1** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	警告	基本配置配置为信任系统证书。
2	*	高危	基本配置配置为信任用户安装的证书。

证书安全分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **1** | 警告: **15** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	App 链接 assetlinks.json 文件未找到 [android:name=com.acceptomobile.common.ui.start.StartActivity] [android:host=https://eg.coupang.acceptto.com]	高危	App Link 资产验证 URL （https://eg.coupang.acceptto.com/.well-known/assetlinks.json） 未找到或配置不正确。（状态代码：None）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify="true"] 启用验证来验证 App Link 网域。
3	Activity设置了 TaskAffinity属性 (com.acceptomobile.common.ui.start.StartActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
4	Activity (com.acceptomobile.common.ui.start.StartActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity设置了 TaskAffinity属性 (com.acceptomobile.common.ui.splash.SplashActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名

6	Activity设置了TaskAffinity属性 (com.accepttomobile.common.ui.MainActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
7	Activity设置了TaskAffinity属性 (com.accepttomobile.common.ui.notification.NotificationActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
8	Activity设置了TaskAffinity属性 (com.accepttomobile.common.ui.lock.PasscodeActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
9	Activity设置了TaskAffinity属性 (com.accepttomobile.basic.BasicModeActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
10	Service (com.accepttomobile.common.wear.WearableReceiverService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
12	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
13	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
14	Service (com.assaabloy.mobilekeys.api.ce.HceService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_NFC_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

15	Broadcast Receiver (no.nordicsemi.android.support.v18.scanner.PendingIntentReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
16	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
17	高优先级的Intent （500） - {1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

</> 安全漏洞检测

高危: **3** | 警告: **9** | 信息: **3** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
2	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
3	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
4	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
5	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
6	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限

7	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
9	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
10	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
11	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
12	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
13	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
14	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
15	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

16	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
17	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00204	获取默认铃声	信息收集	升级会员：解锁高级权限

00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00029	动态初始化类对象	反射	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.READ_PHONE_STATE
其它常用权限	14/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET com.google.android.c2dm.permission.RECEIVE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_BACKGROUND_LOCATION android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_WIFI_STATE android.permission.AUTHENTICATE_ACCOUNTS com.google.android.gms.permission.ACTIVITY_RECOGNITION com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息

www.rfc-editor.org	安全	否	**IP地址:** 172.67.31.145 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
mfa.arculix.com	安全	否	No Geolocation information available.
dev-transport.mobilekeys.assaabloy.net	安全	否	No Geolocation information available.
docs.secureauth.com	安全	否	**IP地址:** 3.169.252.124 **国家:** 美国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.627499 **经度:** -122.340199 **查看:** Google 地图
secureauth.com	安全	否	**IP地址:** 107.178.240.159 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 奥斯丁 **纬度:** 30.271158 **经度:** -97.741699 **查看:** Google 地图
yaml.org	安全	否	**IP地址:** 185.199.110.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
eg.coupang.acceptto.com	安全	否	**IP地址:** 3.39.50.125 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
mfa.arculix.dev	安全	否	No Geolocation information available.
demo-transport.mobilekeys.assaabloy.net	安全	否	**IP地址:** 206.17.82.228 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 圣地亚哥 **纬度:** 32.894405 **经度:** -117.200951 **查看:** Google 地图
decide.mixpanel.com	安全	否	**IP地址:** 107.178.240.159 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

tools.ietf.org	安全	否	**IP地址:** 3.234.115.250 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.151.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
transport.mobilekeys.assaabloy.net	安全	否	**IP地址:** 3.234.115.250 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
dashboard.bugfender.com	安全	否	**IP地址:** 185.206.63.63 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
test-seos-mobile-services.api.assaabloy.com	安全	否	**IP地址:** 18.205.121.203 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
mfa.acceptto.com	安全	否	**IP地址:** 35.201.97.85 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
secureauth-prm-sagpservice.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
safecurve.cr.yp.to	安全	否	**IP地址:** 131.193.32.108 **国家:** 美国 **地区:** 伊利诺伊州 **城市:** 内珀维尔 **纬度:** 41.771000 **经度:** -88.153046 **查看:** Google 地图

seostsm-acceptance-alb-2077998301.us-east-1.elb.amazonaws.com	安全	否	No Geolocation information available.
m2m.acceptto.net	安全	否	**IP地址:** 34.205.150.129 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224361 **经度:** 121.468948 **查看:** 高德地图
www.usenix.org	安全	否	**IP地址:** 23.185.0.4 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.792030 **经度:** -122.406353 **查看:** Google 地图
eg-dev.apac.acceptto.us	安全	否	**IP地址:** 13.125.23.63 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
uaf.acceptto.com	安全	否	No Geolocation information available.
fido2.acceptto.com	安全	否	**IP地址:** 40.121.176.151 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
itsme-localization.s3-us-west-2.amazonaws.com	安全	否	**IP地址:** 52.92.190.226 **国家:** 美国 **地区:** 俄勒冈 **城市:** 博德曼 **纬度:** 45.839859 **经度:** -119.700577 **查看:** Google 地图
api.bugfender.com	安全	否	**IP地址:** 31.170.103.43 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图

api.mixpanel.com	安全	否	**IP地址:** 107.178.240.159 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
test-transport.mobilekeys.assaabloy.net	安全	否	**IP地址:** 10.3.240.63 **国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看:** Google 地图
aiml-dashboard-development.herokuapp.com	安全	否	**IP地址:** 174.129.128.48 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
staging-transport.mobilekeys.assaabloy.net	安全	否	**IP地址:** 44.216.23.234 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
dev.eguardian.io	安全	否	**IP地址:** 3.218.41.194 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
seos-mobile-services.api.assaabloy.com	安全	否	**IP地址:** 18.205.121.203 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• http://creativecommons.org/publicdomain/zero/1.0/ • https://answers.io/terms • https://fabric.io/terms • https://raw.githubusercontent.com/booncol/Pulsator4Droid/master/LICENSE • http://www.boundycastle.org/licence.html • http://fabric.crashlytics.com/terms/terms-of-service.pdf	自研引擎-A
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	vb/b.java

• https://mfa.acceptto.com • https://m2m.acceptto.net • https://dev.eguardian.io • https://mfa.arculix.com • https://eg-dev.apac.acceptto.us/ • https://mfa.arculix.dev • https://eg.coupang.acceptto.com/	com/accepttomobile/common/w0.java
• https://tools.ietf.org/html/rfc7518#section-3.4 • https://tools.ietf.org/html/rfc7518#section- • https://tools.ietf.org/html/rfc7518#section-3.3 • https://tools.ietf.org/html/rfc7518#section-3.2	io/jsonwebtoken/SignatureAlgorithm.java
• https://aiml-dashboard-development.herokuapp.com/ • https://aiml-dashboard-development.herokuapp.com/api/v1/' • http://aiml-dashboard-development.herokuapp.com/api/v1/'	kd/k.java
• https://staging-transport.mobilekeys.assaabloy.net/transportservice/ • https://seostsm-acceptance-alb-2077998301.us-east-1.elb.amazonaws.com/transportservice/ • https://transport.mobilekeys.assaabloy.net/transportservice/ • https://test-transport.mobilekeys.assaabloy.net/transportservice/ • https://dev-transport.mobilekeys.assaabloy.net/transportservice/ • https://demo-transport.mobilekeys.assaabloy.net/transportservice/	mmmmmm/bbgbgb.java
• https://fido2.acceptto.com/	com/accepttomobile/common/ItsMeApplication.java
• https://dashboard.bugfender.com	u8/a.java
• https://%s/%s/%s	kg/c.java
• https://seos-mobile-services.api.assaabloy.com/mobile-statistics • https://test-seos-mobile-services.api.assaabloy.com/mobile-statistics	mmmmmm/yyyyyt.java
• https://uaf.acceptto.com/v1/public/	x3/l.java
• https://plus.google.com/	ec/r0.java
• https://mfa.acceptto.com	com/acceptto/android/sdk/api/license/ItsMeLicense.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	of/r.java
• https://www.rfc-editor.org/rfc/rfc7518.html#section-2	io/jsonwebtoken/impl/lang/BigIntegerUBytesConverter.java
• https://www.rfc-editor.org/rfc/rfc8037.html#section-3.2	io/jsonwebtoken/impl/security/EdSignatureAlgorithm.java
• https://www.rfc-editor.org/rfc/rfc7518.html#section-3.4	io/jsonwebtoken/impl/security/EcSignatureAlgorithm.java
• https://safecurves.cr.yp.to/twist.html	io/jsonwebtoken/impl/security/EcPublicJwkFactory.java
• https://www.rfc-editor.org/rfc/rfc8037#section-3.1	io/jsonwebtoken/impl/security/EcdhKeyAlgorithm.java
• https://www.rfc-editor.org/rfc/rfc7518.html#section-	io/jsonwebtoken/impl/security/DefaultRsaKeyAlgorithm.java
• https://tools.ietf.org/html/rfc7518#section-3.2	io/jsonwebtoken/impl/security/DefaultMacAlgorithm.java

• https://github.com/jwtk/jjwt#custom-json-processor • https://github.com/jwtk/jjwt#json-jackson-custom-types	io/jsonwebtoken/impl/DefaultClaims.java
• https://tools.ietf.org/html/rfc7518#section-3.2	io/jsonwebtoken/security/Keys.java
• https://secureauth.com/	fj/a.java
• https://mfa.acceptto.com	d4/a.java
• https://api.bugfender.com/	i8/a.java
• https://www.rfc-editor.org/rfc/rfc7518.html#section-4.1 • https://www.rfc-editor.org/rfc/rfc7515.html#section-4.1.11 • https://tools.ietf.org/html/rfc7518#section-3.6 • https://www.rfc-editor.org/rfc/rfc7516.html#section-4.1.2 • https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-pellegrino.pdf • https://www.rfc-editor.org/rfc/rfc7516.html#section-4.1.1 • https://www.rfc-editor.org/rfc/rfc7515.html#section-4.1.1 • https://www.rfc-editor.org/rfc/rfc7518.html#section-3.6	io/jsonwebtoken/impl/DefaultJwtParser.java
• https://aiml-dashboard-development.herokuapp.com/ • https://aiml-dashboard-development.herokuapp.com/api/v1/' • http://aiml-dashboard-development.herokuapp.com/api/v1/'	t5/k.java
• https://www.rfc-editor.org/rfc/rfc7518.html#section-3.2	io/jsonwebtoken/impl/security/SecretJwkFactory.java
• https://secureauth.com/	gi/b.java
• https://tools.ietf.org/html/rfc7518#section-	io/jsonwebtoken/impl/security/RsaSignatureAlgorithm.java
• https://itsme-localization.s3-us-west-2.amazonaws.com	com/accepttomobile/common/localization/f.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	vf/f.java
• https://api.mixpanel.com/engage • https://decide.mixpanel.com/decide • https://api.mixpanel.com/track?ip= • https://api.mixpanel.com/groups	com/mixpanel/android/mpmetrics/i.java
• https://www.rfc-editor.org/rfc/rfc7518.html#section-6.3.2	io/jsonwebtoken/impl/security/RsaPrivateJwkFactory.java
• https://yaml.org/spec/1.1/#id934537	org/yaml/snakeyaml/DumperOptions.java
• 4.8.1.2 • https://www.rfc-editor.org/rfc/rfc7518.html#section-4.8.1.2	io/jsonwebtoken/impl/security/Pbes2HsAkwAlgorithm.java
• https://secureauth-com-sagpservice.firebaseio.com • https://docs.secureauth.com/help/en/secureauth-authenticate-app-user-guide.html	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://secureauth-com-sagpservice.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （https://firebaseremoteconfig.googleapis.com/v1/projects/567393951382/namespaces/firebase:fetch?key=AIzaSyAC2sPRyQZ2OJ_LF11x3UD7tDB28k9DQKc） 已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件，库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Android BLE Scanner Compat library	NordicSemiconductor	Scanner Compat 库解决了在 Android 上扫描 BLE 设备的问题。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

追踪器

名称	类别	网址
Bugfender	Analytics, Crash reporting	https://reports.exodus-privacy.eu.org/trackers/233
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

密钥凭证

可能的密钥

谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "AIzaSyCm6qW8icucXnfdxyoUYQcEO49AhUcbzME"
"about_cognitive_authenticator" : "AB0002"
"auth_before_pair_biometric_authenticate_title" : "SP0011"
"biometrics_authentication_not_strong_enough" : "ES0125"
"biometrics_authentication_too_many_attempts" : "ES0126"
"com.google.firebase.crashlytics.mapping_file_id" : "95b8f769b32741599facde76cfc2c07e"
"fido_authenticate_to" : "FS0030"
"fido_fido_authenticator" : "FS0004"
"fido_now_you_can_enable_a_fido2_pin_biometric_authenticator_inside_it_sme_and_authorize_your_mfa_requests" : "FS0005"
"fido_please_authenticate_with_biometrics" : "FS0022"
"fido_row_authenticate" : "FS0018"
"fido_would_you_like_to_enable_acceptto_s_fido_authenticator" : "FS0006"
"fido_your_acceptto_fido_authenticator_has_been_registered_successfully" : "FS0017"
"firebase_database_url" : "https://secureauth-com-sagpservice.firebaseio.com"
"google_api_key" : "AIzaSyAC2sPRyQZ2OJ_LF11x3UD7tDB28k9DQKc"
"google_app_id" : "1:567393951382:android:b650293461019f38"
"google_crash_reporting_api_key" : "AIzaSyAC2sPRyQZ2OJ_LF11x3UD7tDB28k9DQKc"
"hid_key_office_door" : "HK0001"
"mfa_authenticate_to" : "MF0004"
"mirana_secrets_amount_of_data_sent" : "MI0014"
"mirana_secrets_angle_delta" : "MI0002"
"mirana_secrets_end_now" : "MI0015"
"mirana_secrets_latest_notification_received_at" : "MI0005"
"mirana_secrets_notes_record" : "MI0011"
"mirana_secrets_location_lat_lon" : "MI0012"
"mirana_secrets_records_count" : "MI0016"
"mirana_secrets_screen_title" : "MI0001"
"mirana_secrets_share_str" : "MI0008"
"mirana_secrets_time_iso_utc" : "MI0003"
"mirana_secrets_time_ms" : "MI0013"
"mirana_sync_authorities" : "us.acceptto.mirana.syncadapter.provider"

"profile_auth_profile" : "DC0011"
"profile_v3_auth_profile" : "DC0015"
"quick_access_header_authentication_methods" : "QA0002"
"quick_access_header_force_authentication" : "QA0006"
"settings_dialog_are_you_sure_you_want_to_unpair_your_device_you_will_no_longer_be_able_to_use_it_for_it_sme_authentication" : "SE0014"
"sso_detail_dialog_remove_session" : "SD0006"
"sso_no_active_sessions" : "SO0003"
"start_offline_authenticator" : "LS0005"
"start_system_requirements_secret_key_not_hardware_backed" : "SS0005"
"token" : "Token:"
"totp_manual_key" : "TA0006"
"totp_manual_username" : "TA0005"
"username" : "Username"
"vault_password" : "VS0006"
"vault_please_enter_password" : "VS0004"
"vault_your_password_in_your_hand" : "VS0002"
"workstations_sorting_username" : "WS0014"
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6d63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
RtQsRUaCaDLvh8bvSWcUmajSPfdo2YeP
85053bf24bba75239b16a601d9387e17
e054eb924eacca0bf94379f8f6035177
5c3e45889c6eee60aa97e47174e4654f
5c320f72a95ae1fd8ca04ca71606e415
962eddcc369cba7eb240ee6b6a126d9346e38c5
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
8d5155894229d5e689ee01e6018a237e2cae64cd
82c62205f0ef0e4956023a8
3a5d2748bec6cb161e322f8d8b1b13f8
818dd5cb7a3dfbb3eecc94634dabba70
520bc9aa3899e8154622a96a5b342b5d

ff29052e-75b8-40cb-b41c-2404a5a31a53
9747ba803239cf475ca29faa108fe278
4747474752450653d7387d8f42698bfa3557f0d9e791a83231d0a8aec6f69d70
2c94422adaeef51dfab90706db997894
c5c8a58e2309dd4f500de460a0ace695c579c4bc8f693e91d66a7d56c1d3cf58
47474747487408fb703a79fe63c967f7120da0fe92b5b2a2c43c303524533f19
MIICEjCCAbgCCQDJPP0w3hWewzAKBggqhkjOPQQDAjCBkDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk9SMREwDwYDVQQHDAhOb21haGFuZDERMA8GA1UECgwIQWNjZXB0dG8xETAPBgNVBAsMCEFjY2VwdHRvMREwDwYDVQQDDAhBY2NlcHR0bzEoMCYGCSqGSIb3DQEJARYZbWFndC5yb3Nhbmlv QGFjY2VwdHRvLmNvbTAeFw0xODA1MDIwNDU1MDZaFw0yODA0MjkwNDU1MDZaMIGQMQswCQYDVQQGEwJVUzELMAkGA1UECAwCT1IxETAPBgN VBAcMCFBvcnRsYW5kMREwDwYDVQQKDAhBY2NlcHR0bzERMA8GA1UECwwIQWNjZXB0dG8xETAPBgNVBAMMCEFiY2NwdHRvMSgwJgYJKoZIhvcNA QkBFhltYXR0LnJvc2FuaW9AYWNjZXB0dG8uY29tMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEAjPvAFRLCz3PiQXJIxPBbOna9IFPkmMgbTrp+UPzmulUD KJaMjlQrspfVcdJs+0QOSVLQ2BRKFhe29MTBZRlwzAKBggqhkjOPQQDAgNIADBFAiEA6rSGiWOjPBOjZUFs81qiHOxzLCMnTdAfD3H+LWzJyLECIA8wQEJ7 OFnq6ZfGiK2qVUkGSnQB75yns7EDmsGeOV11
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b3a2e2935630e1c2062354d0da20a1c416e50be794ca4
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
9760508f15230bccb292b982a2eb840bf0581cf5
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEAjPvAFRLCz3PiQXJIxPBbOna9IFPkmMgbTrp+UPzmulUDKJaMjlQrspfVcdJs+0QOSVLQ2BRKFhe29MTBZRlww==
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fec7107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1beea519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
470fa2b4ae81cd56ecbcda9735803434cec591fa
xJXZd/zR0io4+XWtcwbtnyYutpO4NX7DhE2xLg4=
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d57aea063e5a1f6a7064f316933a346d7f529252
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3780b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c1a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
a5f769eb00efe3ea64404c96c2b4fc3
ad120db1f5bce5b77a39da92b11ba477a7fcb180e2c0d9248728a5c80111e9e4
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
xBkDPNxUEiMRX5yPP2WqvCR4Grb8GZQqrKNyC0Y
14201c8e11cc4fda1c9c98d5d7b72f6d5404a8f233c9fc8b1930bd8f3fb547b9
d6149640291079l465933c3d81ab4f80
acce6770-163d-11e8-b642-0ed5f89f718b
-11e8-b642-0ed5f89f718b

GooglePlay应用信息

标题: SecureAuth Authenticate

评分: 3.3960395 **安装:** 500,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** secureauth.android.token

开发者信息: SecureAuth, SecureAuth, None, http://www.secureauth.com, support@secureauth.com,

发布日期: 2013年3月28日 **隐私政策:** Privacy link

关于此应用:

SecureAuth Authenticate是一种现代的移动应用程序，可验证您的身份，以便您可以安全地访问您的应用程序。 SecureAuth Authenticate支持针对个人，工作或学校应用程序和帐户的多因素身份验证（MFA）。身份验证器生成两位数身份验证（2FA）流中常用的6位一次性密码/令牌（OTP代码）。 SecureAuth身份验证供个人使用 两步验证可确保您的个人帐户不被帐户接管。通过SecureAuth Authenticate，您可以保护自己的Gmail，Outlook，LinkedIn，Dropbox和数以千计的其他云应用程序。 个人特色： •支持多个帐户 •快速QR码设置 •无需Wi-Fi或数据连接即可离线工作 •可以安装到任何基于Wear OS的设备上。 SecureAuth认证以用于商业 与企业部署中的SecureAuth IDaaS配对时，SecureAuth Authenticate可提供其他强大的身份验证优势。该应用程序旨在与自适应/无密码身份验证一起使用，适用于云/ SaaS和本地应用程序单点登录（SSO）方案。 关键业务功能： •推送通知–提示批准/拒绝需要MFA的登录 •符号到接受–高安全性提示，要求用户匹配特定的符号 •解锁检测–禁用电话锁定保护时的安全保护 •防克隆–将电话操作系统克隆到另一部电话时的安全保护 •PIN码保护–提示输入PIN码以显示OTP码 •脱机模式–为受MFA保护的Windows或MacOS登录生成OTP代码 •QR码或激活链接注册–配置应用程序的便捷方法 入门 请按照您要保护的应用中的2FA或MFA设置步骤进行操作。扫描QR码或输入设置代码后，您的帐户将被设置为2FA。 请访问https://www.secureauth.com/secureauth-authenticate以开始使用。

免责声明及风险提示: