MoGua

银联可信服务安全组件 01.00.96.APK 分析报告

APP名称:	银联可信服务安全组件

包名:	com.unionpay.tsmservice
域名线索:	12条
URL线索:	13条
邮箱线索:	0条
分析日期:	2025年6月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 银联可信安全服务组件（三星、魅族）01.00.96.apk

文件大小: 17.06MB
MD5值: 4fba55f305edcfc03e5a7f9b925715ed
SHA1值: 5bf633b6bfb1022ba9d778f8ddb0d9b6f0f06c8a
SHA256值: 92e3c47e1f49e116131a23522f85a5d0cf5406cf49165b1c006399a21812d521

APP 信息

App名称: 银联可信服务安全组件
包名: com.unionpay.tsmservice
主活动Activity:
安卓版本名称: 01.00.96
安卓版本: 97

域名线索

域名	服务器信息
onekey.cmpassport.com	**IP**: 120.197.235.28 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
cupiv.95516.com	**IP**: 58.220.75.72 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
unilog.wostore.cn	**IP**: 116.128.209.129 **所属国家**: China **地区**: Beijing **城市**: Beijing

	纬度: 39.907501 **经度**: 116.397102
id6.me	IP: 42.123.77.138 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
collect.ux.21cn.com	IP: 222.93.106.185 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311365 **经度**: 120.617691
opencloud.wostore.cn	IP: 116.128.209.136 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mobile.unionpay.com	没有服务器地理信息.
config2.cmpassport.com	IP: 112.33.111.251 **所属国家**: China **地区**: Anhui **城市**: Hefei **纬度**: 31.863815 **经度**: 117.280830
log2.cmpassport.com	IP: 36.138.255.61 **所属国家**: China **地区**: Gansu **城市**: Lanzhou **纬度**: 36.056690 **经度**: 103.792221

onekey2.cmpassport.com	**IP**: 120.197.235.28 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
acpstatic.95516.com	**IP**: 117.24.10.73 **所属国家**: China **地区**: Fujian **城市**: Quanzhou **纬度**: 24.913891 **经度**: 118.585831
h5hosting-drcn.dbankcdn.cn	**IP**: 106.38.242.113 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
https://id6.me/auth/preauth.do	cn/com/chinatelecom/gateway/lib/c/a.java
https://collect.ux.21cn.com/collect/custom/accountMsg	cn/com/chinatelecom/gateway/lib/b/d.java
https://cupiv.95516.com/usp/tx/9002	com/nantian/operators/sdk/OperatorsSDKManager.java
https://cupiv.95516.com/usp/tx/getTokenErro	com/nantian/operators/sdk/OperatorsSDKManager.java
https://cupiv.95516.com/usp/tx	com/nantian/operators/sdk/utils/HttpUtils.java

https://log2.cmpassport.com:9443/log/logReport	com/cmic/sso/sdk/d/p.java
https://onekey2.cmpassport.com/unisdk	com/cmic/sso/sdk/d/p.java
http://onekey.cmpassport.com/unisdk	com/cmic/sso/sdk/d/p.java
https://config2.cmpassport.com/client/uniConfig	com/cmic/sso/sdk/b/c/a.java
https://config2.cmpassport.com/client/uniConfig	com/cmic/sso/sdk/b/a/a.java
https://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/login/c/h.java
https://unilog.wostore.cn:18080/logserver/account/sdknopasswd	com/unicom/xiaowo/login/c/h.java
https://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/login/c/e.java
https://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/login/c/f.java
https://h5hosting-drcn.dbankcdn.cn/cch5/huaweipaycdn/bankCard_hwpSupportList/index.html	com/unionpay/mobile/android/utils/j.java
https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\	com/unionpay/mobile/android/utils/c.java
https://acpstatic.95516.com/gw/app/resources/images/payapps/pay_app_cqp.png\	com/unionpay/mobile/android/pro/views/g.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 2 个唯一证书
主题: C=CN, ST=Shanghai, L=Shanghai, O=China UnionPay Co. Ltd, OU=China UnionPay, CN=China UnionPay
签名算法: rsassa_pkcs1v15
有效期自: 2020-09-24 07:04:17+00:00
有效期至: 2060-09-14 07:04:17+00:00
发行人: C=CN, ST=Shanghai, L=Shanghai, O=China UnionPay Co. Ltd, OU=China UnionPay, CN=China UnionPay
序列号: 0x301f5d84
哈希算法: sha384
md5值: 611fd45661a409cf0dc79e464fa3b5eb
sha1值: 1003cfe4619596ba678069eb7e47c494ef41bde6
sha256值: f72023e4f9012d5074238f25b85aae4f3730bfb7dbb49aca3f735d5856c03345
sha512值: 071b9a4061fc9084cab703477b7765e31476e551e1818127e2412dc5e0f9bf4d4d36ee10a462ab8e522a8589003eaba9565beef919b0befb495f3e07346365e5
主题: C=CN, ST=Shanghai, L=Shanghai, O=China UnionPay Co. Ltd, OU=China UnionPay, CN=China UnionPay
签名算法: rsassa_pkcs1v15
有效期自: 2011-05-20 02:15:18+00:00
有效期至: 2041-05-12 02:15:18+00:00
发行人: C=CN, ST=Shanghai, L=Shanghai, O=China UnionPay Co. Ltd, OU=China UnionPay, CN=China UnionPay
序列号: 0x4dd5ceb6
哈希算法: sha1
md5值: f866bf76d5423c5de1b53b93a789f652
sha1值: 536c79b93acfbea950ae365d8ce1aef91fea9535
sha256值: 5f6b3d22859624a8de36f95d03ae2ff7581a1daabb230c62aed9470a54414845
sha512值: daa6f907431e05fe260dbc5aa1ebfa0e0bc821b6f1ff42095e2867a1f227cca61ac4e83dfd745a194bd2f15c435c28806ce17eeeb787a27240cbffd232af5250
公钥算法: rsa
密钥长度: 1024
指纹: 42b7fb47f4d4f45a6f948179a0987fc4439b4e91c6aa8b3c5e92388f4aebbcbd
公钥算法: rsa
密钥长度: 3072
指纹: 131a2167ee70b14f7447464f222e590a5ebe5203cdbd26b1c941e4c056be5fe7

🔑 硬编码敏感信息

可能的敏感信息
"decrypt_session_key_fail" : "decrypt session key fail"

"real_name_authentication" : "实名认证"
"real_name_authentication_desc" : "用户完成实名认证，无需输入银行卡号等信息，即可快捷绑卡。信息仅用于实名认证，银联保障信息安全。"
"real_name_authentication_step_desc" : "只需2步即可完成实名认证 填写姓名、身份证号>人脸识别"
"sessionkey_area_is_missing" : "sessionkey area is missing"
"start_real_name_authentication" : "开始实名认证"
"decrypt_session_key_fail" : "decrypt session key fail"
"sessionkey_area_is_missing" : "sessionkey area is missing"
"decrypt_session_key_fail" : "не удалось расшифровать ключ"
"sessionkey_area_is_missing" : "область ключа сеанса отсутствует"

加壳分析

加壳类型	**所属文件**
登陆摸瓜网站后查看	

第三方插件

名称	**分类**	URL**链接**
登陆摸瓜网站后查看		

登陆其他网站后查看		

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
com.nxp.nfceeapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference

com.samsung.android.spay.permission.USE_SDK	未知	Unknown permission	Unknown permission from android reference
com.vendor.permission.TSM	未知	Unknown permission	Unknown permission from android reference
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。
com.tencent.mtt.extension.Player	未知	Unknown permission	Unknown permission from android reference
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
com.vivo.systemui.notification.permission.dialog.access.permission	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.unionpay.uppay.PayActivity	Schemes: uppay://, uppow://,
com.unionpay.tsmservice.activity.QuickPassFundActivity	Schemes: uptsm://, Hosts: tsmservice.unionpay.com, Paths: /quickpassfund,