



香港一卡通 1.1.15.APK 分析报告



APP名称:

香港一卡通

包名: com.cmbchina.mbankhk

域名线索: 31条

URL线索: 16条

邮箱线索: 0条

分析日期: 2025年8月2日

分析平台: [摸瓜APK反编译平台](#)

文件名: 香港一卡通手机银行_1.1.15_Apkpure.apk
文件大小: 155.45MB
MD5值: 9480e5ba65169903fdfe5a6c6e39c519
SHA1值: 68a25fcca54de8d34263fadd176a751aa24a0d92
SHA256值: 372f3eec25afca457f1d2f416519361f1c89a3ca958337638e82d4595147f85a

i APP 信息

App名称: 香港一卡通
包名: com.cmbchina.mbankhk
主活动Activity: com.cmbchina.cmf.ui.splash.SplashActivity
安卓版本名称: 1.1.15
安卓版本: 32

🔍 域名线索

域名	服务器信息
bit.ly	IP: 67.199.248.10 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009
grs.dbankcloud.eu	没有服务器地理信息.
data-dre.push.dbankcloud.com	IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532

store-dra.hispace.dbankcloud.com	IP: 222.73.142.42 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
store-at-dre.hispace.dbankcloud.com	没有服务器地理信息.
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
metrics.dt.dbankcloud.ru	IP: 159.138.204.140 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
g.co	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
	IP: 49.4.40.185 所属国家: China 地区: Guangdong

grs.dbankcloud.cn	城市: Guangzhou 纬度: 23.127361 经度: 113.264572
angular.io	IP: 151.101.65.195 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
m.cmbchina.com	IP: 116.7.243.51 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
store-drru.hispace.dbankcloud.com	IP: 159.138.205.168 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
data-drcn.push.dbankcloud.com	IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
central.jaf.cmbchina.cn	没有服务器地理信息.
grs.dbankcloud.com	IP: 113.201.107.90 所属国家: China 地区: Shaanxi 城市: Baoji 纬度: 34.353611

	经度: 107.375275
cmb-index.weijuju.com	没有服务器地理信息.
market.cmbchina.com	IP: 125.39.103.211 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
data-drru.push.dbankcloud.com	IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
store-dre.hispace.dbankcloud.com	IP: 222.73.142.45 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.baidu.com	IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
play.google.com	IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547

grs.dbankcloud.asia	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
store-drcn.hispace.dbankcloud.cn	IP: 111.202.16.109 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
data-dra.push.dbankcloud.com	IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
metrics1.data.hicloud.com	IP: 111.202.17.12 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.platform.dbankcloud.ru	没有服务器地理信息.
metrics2.data.hicloud.com	IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast'

metrics5.data.hicloud.com	城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
material.angular.io	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
appgallery.cloud.huawei.com	IP: 121.36.118.136 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://m.cmbchina.com	Mogua Engine V1
https://play.google.com/store/apps/details?id=	Mogua Engine V1
https://appgallery.cloud.huawei.com	Mogua Engine V1
https://metrics1.data.hicloud.com:6447	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2
https://metrics2.data.hicloud.com:6447	Mogua Engine V2

https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2
https://grs.platform.dbankcloud.ru	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2
https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/	Mogua Engine V2
https://data-drcn.push.dbankcloud.com	Mogua Engine V2
https://data-dra.push.dbankcloud.com	Mogua Engine V2
https://data-dre.push.dbankcloud.com	Mogua Engine V2
https://data-drru.push.dbankcloud.com	Mogua Engine V2
https://store-drcn.hispace.dbankcloud.cn/hwmarket/api/	Mogua Engine V2
https://store-dra.hispace.dbankcloud.com/hwmarket/api/	Mogua Engine V2
https://store-dre.hispace.dbankcloud.com/hwmarket/api/	Mogua Engine V2
https://store-drru.hispace.dbankcloud.com/hwmarket/api/	Mogua Engine V2
https://metrics1.data.hicloud.com:6447	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2

https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://metrics.dt.dbankcloud.ru	Mogua Engine V2
https://material.angular.io/guide/theming	Mogua Engine V2
http://cmf/zhaohu	Mogua Engine V2
http://cmf/clipboard	Mogua Engine V2
http://www.baidu.com	Mogua Engine V2
http://cmf/secureStorage	Mogua Engine V2
http://cmf/deviceInfo	Mogua Engine V2
http://cmf/keyboard	Mogua Engine V2
http://cmf/statusbar	Mogua Engine V2
http://cmf/topBarUI	Mogua Engine V2
http://g.co/ng/security	Mogua Engine V2
https://angular.io/docs/ts/latest/api/common/index/NgFor-directive.html	Mogua Engine V2
http://bit.ly/IWukam	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1999/xhtml	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/XML/1998/namespace	Mogua Engine V2

http://www.w3.org/2000/xmlns/	Mogua Engine V2
http://central.jaf.cmbchina.cn:80/artifactory/api/npm/group-npm/@za30/zhaohu-im/-/@za30/zhaohu-im-1.9.24.tgz	Mogua Engine V2
http://a	Mogua Engine V2
http://a/c%20d	Mogua Engine V2
https://market.cmbchina.com/MPage/online/210910112740454/cmbhk.html	Mogua Engine V2
http://cmbls/functionjump	Mogua Engine V2
https://cmb-index.weijuju.com/4/index.html	Mogua Engine V2
https://www.baidu.com	Mogua Engine V2
https://market.cmbchina.com/MPage/online/210910112740454/cmbhk.html	Mogua Engine V2
https://market.cmbchina.com/personal/webapp/html/docs/license/service-detail.html	Mogua Engine V2
https://market.cmbchina.com/MPage/online/210806152450230/vtef.html	Mogua Engine V2
https://market.cmbchina.com/MPage/online/210910112740454/cmbhk.html	Mogua Engine V2

 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 1 个唯一证书
主题: C=China, ST=Hong Kong, L=Hong Kong, O=CMB, OU=CMBHK, CN=CMB Hong Kong
签名算法: rsassa_pkcs1v15
有效期自: 2019-05-06 00:57:06+00:00
有效期至: 2044-04-29 00:57:06+00:00
发行人: C=China, ST=Hong Kong, L=Hong Kong, O=CMB, OU=CMBHK, CN=CMB Hong Kong
序列号: 0x786ec7ce
哈希算法: sha256
md5值: fbe455aaca685d49fd3dbee6c8150cc0
sha1值: 47796999a6baa19bd5cce742d15f99534b6a2c26
sha256值: f1f7ce78028897015c42c0f2be82f4bd3ac6e451fd167061246cc18c52cfe84c
sha512值: b0f5ee36d99f0a9fc0d1525094c5ce1f2e42acb0b70f1ea5d60072cae3cbd22bfac934e0effca6ee4a6f5105a68c230a82593ed91fded7129bcf1015bcf5e98f
公钥算法: rsa
密钥长度: 2048
指纹: 87f82e87136390c9559321325a07957933761192faa3b26cfda27c77756a7a56

硬编码敏感信息

可能的敏感信息
"bank_auth_cancel" : "授权取消"
"bank_auth_failed" : "授权失败"
"bank_auth_param_null" : "传入参数为空"
"bank_auth_waiting" : "正在授权，请耐心等待"
"cancel_more_auth" : "取消"
"face_authorized_msg" : "拒绝人脸识别验证将会无法继续操作，确定拒绝吗？"
... 还有 1 个敏感信息 "取消面容解锁"

"keyboard_secret": "配置安全鍵盤密鑰"
"keyboard_secret_info": "自定义安全键盘密钥不能为空"
"login_bank_auth": "招商银行App快捷登录"
"login_netcom_password": "—网通密码"
"login_pwd": "密码登录"
"login_retry_password": "重试密码登录"
"login_risk_password": "为了您的信息安全，请进行登录密码验证"
"more_auth_btn": "切换账号或登录方式"
"more_auth_verify_btn": "更多"
"netcom_bio_login_auth_failed": "指纹验证失败，请稍后重试"
"netcom_bio_login_bff_auth_failed": "指纹已失效，请采用其他方式登录成功后重新设置"
"netcom_login_auth_page_title": "登录认证"
"safe_keyboard_secret_title": "请输入安全键盘密钥"
"keyboard_secret": "配置安全鍵盤密鑰"
"keyboard_secret_info": "自定義安全鍵盤密鑰不能為空"
"safe_keyboard_secret_title": "請輸入安全鍵盤密鑰"
"keyboard_secret": "配置安全键盘密钥"
"keyboard_secret_info": "自定义安全键盘密钥不能为空"

"safe_keyboard_secret_title" : "请输入安全键盘密钥"

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		

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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.READ_PRIVILEGED_PHONE_STATE	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
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.WAKE_LOCK	正	防止手机睡	允许应用程序防止手机进入睡眠状态

	常	眠	
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
com.cmbchina.mbankhk.permission.MIPUSH_RECEIVE	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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.huawei.pushagent.permission.RICHMEDIA_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知	在华为手机的应用程序启动图标上显示通知计数或徽章。

		计数	
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.launcher3.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知	在三星手机的应用程序启动图标上显示通知计数或徽章。

		计数	
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。

com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.cmbchina.mbankhk.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.cmbchina.mbankhk.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.cmbchina.mbankhk.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.cmbchina.mbankhk.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.cmbchina.cmf.plugins.netcom.banklogin.ReceiveDataActivity	Schemes: cmfdemo://,

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