ICS 35.240.01
CCS L70

团　　体　　标　　准

T/ISC 0017—2022

移动互联网应用程序 SDK 安全技术要求及测试方法

Security technical requirements and test methods of mobile application SDK

2022－08－05 发布　　2022－11－05 实施

中　国　互　联　网　协　会　　发 布

目　　次

前　言

本文件按照GB/T 1.1-2020给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国互联网协会归口。

本文件主要起草单位：中国信息通信研究院、中国电信集团公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、北京腾云天下科技有限公司、深圳市和讯华谷信息技术有限公司、深圳凡泰极客科技有限责任公司、北京贵士信息科技有限公司、每日互动股份有限公司、深圳市网安计算机安全检测技术有限公司、北京数智鑫源科技有限公司

本文件主要起草人：解伯延、王丹辉、钟子呈、江为强、谢玮、陈湉、刘明辉、耿冠和、蔡逆水、张峰、刘畅、徐积森、吴连勇、葛梦莹、陈光炎、马超、史坤坤、梁启鸿、杨涛、任馨怡、张青峰、董霖、郄世杰、方毅、黄伟杰、郑建鹏、任江辉、柯国锋 、宫琦

移动互联网应用程序SDK安全技术要求及测试方法

1 范围

本文件规定了移动互联网程序（App）软件开发工具包（SDK）的开发、运营中的安全要求，并描述了满足这些安全要求的证实方法。

本文件适用于移动互联网应用程序SDK安全测评工作，为相关机构强化测评能力、健全技术手段提供指引，为SDK开发者提升其产品安全水平提供参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动互联网应用程序 mobile internet application

通过预装、下载等方式获取并运行在移动智能终端上，向用户提供服务的应用软件，简称App。

注：本文件中的App，包括移动智能终端预置的App、可以通过网站、应用商店等应用分发平台下载、安装和升级的App，及小程序等基于宿主App平台的应用软件。

3.2

软件开发工具包 software development kit

协助软件开发的软件库，通常包括相关二进制文件、文档、范例和工具的集合，简称 SDK。

3.3

移动互联网应用程序提供者 mobile internet application provider

移动互联网应用程序的所有者或运营者，简称 App 提供者。

3.4

最终用户 end user

在移动终端设备上使用移动互联网应用程序的个人用户，即 App 用户。

4 缩略语

下列缩略语适用于本文件。

SDK：软件开发工具包（Software Development Kit）

App：移动互联网应用程序（Mobile Internet Application）

Demo：展示样本（Demonstration）

5 移动互联网应用程序 SDK 安全要求

5.1 基本安全要求

SDK基本安全要求如下：

a）应确保分发过程具备有效的完整性校验机制，避免提供的代码、资源文件遭篡改。

b）应确保分发包、Demo包内不包含病毒、木马等恶意程序。

c）应避免调试信息函数输出通信日志、关键变量等敏感信息。

d）应避免分发包、Demo包内残留内网URL、测试账号、测试数据等测试信息。

e）应避免嵌入与业务功能无关的插件、代码，或在分发包中私自打包提供其他SDK产品。

f）申请系统权限应遵循最小必要原则，避免索要非实现业务功能所必须的权限。

5.2 数据存储安全要求

SDK数据存储安全要求如下：

a）应对存储于最终用户设备上的含有个人信息、重要数据的文件进行加密（如库表加密、文件加密等），避免被宿主App、其他App、恶意程序等非法访问、篡改。

b）宜对与宿主App或其他本地程序共同处理、使用的数据进行加密处理，并约定安全有效的解密方案，确保数据的合法授权访问。

c）应对存储于最终用户设备上的数字证书文件进行加密，避免数字证书泄露或遭非法篡改。

d）应对存储于最终用户设备上的备份数据进行加密，避免备份数据泄露。

e）应限制本地存储的配置信息、用户偏好等轻量数据读写权限，避免遭其他程序越权访问、篡改。

f）宜限制个人信息、重要数据本地存储时间，确保到期数据自动删除。

g）应避免本地存储去标识化数据与原始标识的对应关系信息，防止相关信息泄露导致去标识化失效。

h）应避免本地存储明文的鉴权信息（如账号、密码等），宜采用加随机盐的哈希值方式存储相关数据，避免用户个人敏感信息泄露。

5.3 数据交互安全要求

SDK与宿主App、服务端数据交互应满足的安全要求如下：

a）应采用安全的传输协议确保SDK与服务端数据交互的机密性、完整性、可用性。

b）涉及个人信息、重要数据传输的场景，应采用HTTPS等加密传输协议或对相关数据单独加密，确保个人信息加密传输。

c）使用HTTPS传输协议时，宜开启SDK与服务端的双向验证机制，确保服务端身份真实性。

d）使用HTTPS自定义证书时，应对服务端主机名进行校验，验证服务端主机身份。

e）应使用安全的加密算法、密钥生成机制，避免使用不安全的加密算法（如RC4、AES ECB或OFB工作模式等），避免加密算法破解。

5.4 重要组件安全要求

SDK使用系统功能组件应满足的安全要求如下：

a) 应在使用组件调用系统功能时确保其配置安全性，避免出现配置不合理导致的安全风险。

b) 应在使用组件调用系统功能时遵循最小必要原则，避免调用与实现业务功能无关的功能。

c) 调用网页视图（WebView）应确保其配置安全性，避免出现配置不合理导致的安全风险。

d) 调用网页视图（WebView）实现与服务端交互时，应符合5.1.3章节各项要求。

e) 宜在调用Intent组件时验证接收方合法性并对参数进行过滤，避免出现越权调用、隐式调用等风险。

f) 宜在调用Intent组件时增加异常捕获机制，避免出现程序崩溃等风险。

5.5 代码及资源文件安全要求

SDK代码及资源文件安全要求如下：

a) 宜采用代码混淆、加固等手段提高逆向分析的难度，降低关键函数、逻辑等泄露风险。

b) 宜对本地存储的so文件进行加固/混淆处理，避免敏感信息泄露。

c) 宜对本地存储的h5资源文件进行加密处理，避免资源文件遭篡改。

d) 如采用资源文件热更新技术，宜对文件解压文件名进行限制，避免更新的资源文件被非法获取。

e) 宜对本地存储的so文件进行地址空间随机化,降低缓冲区溢出攻击风险。

f) 宜对本地存储的so文件进行编译器堆栈保护，避免栈溢出时系统不对程序进行保护。

g) 宜对本地存储的密钥、证书进行加密，避免本地密钥、证书泄露或遭篡改。

h) 宜避免代码内存在硬编码或强耦合的URL地址，避免链接遭篡改。

6 移动互联网应用程序 SDK 安全测试方法

6.1 基本安全测评

编号	基本安全-1
测评项目	SDK 分发缺少完整性校验
风险描述	分发过程缺少完整性校验机制可能导致 App 提供者获取伪造、遭篡改的 SDK 代码。
标准要求	5.1 a)
测评方法	访问 SDK 下载渠道，查验是否提供 hash 值比对、签名证书等完整性校验机制。
测评结果	存在风险：分发渠道提供了完整性校验机制。 未见异常：分发渠道未提供完整性校验机制。

编号	基本安全-2
测评项目	内含恶意程序
风险描述	分发包内含有病毒、木马等恶意程序对 App 提供者、最终用户均可能造成安全威胁。
标准要求	5.1 b)
测评方法	解压缩 SDK 分发包，扫描是否含有病毒、木马等恶意程序。
测评结果	存在风险：分发包内未见病毒、木马等恶意程序。 未见异常：分发包内发现病毒、木马等恶意程序。。

编号	基本安全-3
测评项目	调试日志输出敏感信

风险描述	调试信息函数输出日志可能泄露代码逻辑等敏感信息，导致安全风险。
标准要求	5.1 c)
测评方法	反编译 SDK 代码，查验调试信息函数是否禁用，如未禁用则查验输出日志是否含有敏感信息。
测评结果	存在风险：调试信息函数未禁用，且日志含敏感信息。 未见异常：调试信息函数已禁用，或输出日志不含敏感信息。

编号	基本安全-4
测评项目	残留测试信息
风险描述	残留测试数据可能导致测试服务器地址、测试账号等信息泄露，威胁运维安全。
标准要求	5.1 d)
测评方法	反编译 SDK 代码，查验是否残留服务器地址、测试账号等测试信息。
测评结果	存在风险：代码中发现残留测试信息。 未见异常：代码中未发现残留测试信息。

编号	基本安全-5
测评项目	内嵌无关插件、SDK
风险描述	与业务功能无关的插件、SDK 等可能会携带恶意程序或造成其他安全风险。
标准要求	5.1 e)
测评方法	解压缩 SDK 分发包，查验资源文件中是否存在与业务功能无关的插件、SDK 等。
测评结果	存在风险：分发包内发现与业务功能无关的插件、SDK 等。 未见异常：分发包内未发现与业务功能无关的插件、SDK 等。

编号	基本安全-6
测评项目	索要非必要权限
风险描述	索要与实现 SDK 业务功能无关的非必要权限可能导致合规性风险。
标准要求	5.1 f)
测评方法	核验 SDK 权限声明情况，比照业务功能，判断是否申请与业务功能无关的系统权限。
测评结果	存在风险：申请与业务功能无关的系统权限。 未见异常：未申请与业务功能无关的系统权限。

6.2 数据存储风险测评

编号	数据存储风险-1
测评项目	数据明文存储
风险描述	本地明文存储数据，可能导致个人信息、重要数据等遭非法访问、篡改
标准要求	5.2 a)
测评方法	进入 SDK 本地数据存储路径，查验是否存在明文存储的数据库文件，如有则查验其内容是否存在敏感信息。
测评结果	存在风险：发现明文存储的数据库文件，且内容含敏感信息。 未见异常：未发现明文存储的数据库文件，或内容不含敏感信息。

编号	数据存储风险-2
测评项目	共享数据明文存储
风险描述	SDK 与本地程序共同处理、使用的数据未加密，可能导致数据越权访问风险。
标准要求	5.2 b)
测评方法	进入宿主 App 及 SDK 本地数据存储路径，结合技术文件查阅与开发人员访谈结果，查验是否存在明文存储的共享文件，如有则查验其内容是否存在敏感信息。
测评结果	存在风险：发现明文存储的共享文件，且内容存在敏感信息。 未见异常：未发现明文存储的证书文件，或明文存储的共享文件内未存储敏感信息。

编号	数据存储风险-3
测评项目	数字证书明文存储
风险描述	明文存储的数字证书可能遭窃取、篡改，导致传输数据被截获、伪造传输请求等安全风险。
标准要求	5.2 c)
测评方法	反编译 SDK 代码，查验资源文件中是否存在明文存储的证书文件。
测评结果	存在风险：发现明文存储的证书文件。 未见异常：未发现明文存储的证书文件。

编号	数据存储风险-4
测评项目	备份数据明文存储
风险描述	如 SDK 开启数据备份功能并以明文存储备份数据，可能导致备份数据遭越权访问。
标准要求	5.2 d)
测评方法	反编译 SDK 代码，查验是否开启了数据备份功能，如是则进入 SDK 备份数据存储目录，查验备份数据是否明文存储。
测评结果	存在风险：开启数据备份且备份数据明文存储。 未见异常：未开启数据备份或备份数据加密存储。

编号	数据存储风险-5
测评项目	数据全局可读写
风险描述	如开启轻量数据全局读写权限，可能导致本地存储的配置信息、用户偏好等信息遭越权访问、篡改。
标准要求	5.2 e)
测评方法	查阅 SDK 技术信息，访谈开发人员，查验 SDK 开发过程中是否关闭或限制轻量数据读写权限。
测评结果	存在风险：轻量数据全局可读写权限已开启。 未见异常：轻量数据全局可读写权限未开启。

编号	数据存储风险-6
测评项目	数据超期存储
风险描述	如未限制数据存储周期，可能导致个人信息、重要数据超期存储。
标准要求	5.2 f)

测评方法	查阅 SDK 技术信息，访谈开发人员，查验 SDK 开发过程中是否限制本地数据存储周期，进入 SDK 本地存储路径，查验超出存储期限数据是否删除。
测评结果	存在风险：限制了数据存储期限且到期删除。 未见异常：未限制数据存储期限或到期未删除。

编号	数据存储风险-7
测评项目	标识对应关系本地存储
风险描述	如本地存储去标识化数据与原始标识的对应关系信息泄露，可能导致去标识化失效。
标准要求	5.2 g)
测评方法	结合 SDK 技术信息查阅、开发人员访谈情况，进入 SDK 本地存储路径，查验是否存在本地存储的标识化数据与原始标识的对应关系信息。
测评结果	存在风险：发现本地存储的标识化数据与原始标识的对应关系信息。 未见异常：未发现本地存储的标识化数据与原始标识的对应关系信息。

编号	数据存储风险-8
测评项目	鉴权信息铭文存储
风险描述	如本地明文存储鉴权信息（如账号、密码等），可能导致用户个人敏感信息泄露。
标准要求	5.2 h)
测评方法	结合 SDK 技术信息查阅、开发人员访谈情况，查验 SDK 是否仅存储鉴权信息哈希值，且哈西值计算过程中进行了随机盐添加。
测评结果	存在风险：本地存储明文的用户鉴权信息。 未见异常：未存储明文用户鉴权信息或相关信息为加盐的哈希值。

6.3 数据交互风险测评

编号	数据交互风险-1
测评项目	敏感信息 HTTP 协议传输
风险描述	HTTP 协议通信使用明文传输且不验证通信方的身份及报文完整性，可能导致数据泄露、中间人攻击等安全风险。
标准要求	5.3 a）
测评方法	抓取 HTTP 协议数据包进行分析，查验是否存在明文的个人信息、重要数据等敏感信息。
测评结果	存在风险：发现明文敏感信息使用 HTTP 协议传输。 未见异常：未发现明文敏感信息使用 HTTP 协议传输。

编号	数据交互风险-2
测评项目	敏感信息明文传输
风险描述	明文传输的数据可能遭截获，导致敏感信息泄露。
标准要求	5.3 b）
测评方法	抓取通信流量并分析内容，查验是否可截获明文个人信息、重要数据等敏感信息。
测评结果	存在风险：截获明文敏感信息输。 未见异常：未截获明文敏感信息。

编号	数据交互风险-3
测评项目	HTTPS 未开启双向认证
风险描述	未开启 HTTPS 双向证书验证可能导致加密数据遭劫持、解密，导致数据泄露等风险。
标准要求	5.3 c）
测评方法	配置证书文件并进行流量分析，查验是否使用了 HTTPS 单向认证机制。
测评结果	存在风险：使用 HTTPS 单向认证机制。 未见异常：未使用 HTTPS 单向认证机制。

编号	数据交互风险-4
测评项目	HTTPS 未验证主机名
风险描述	缺少主机名校验机制，SDK 可能与仿冒的服务器建立通信，导致中间人攻击风险。
标准要求	5.3 d）
测评方法	反编译样品文件，查验是否使用了自定义 SSL 证书，如是责则查验 HTTPS 相关设置是否开启主机名校验。
测评结果	存在风险：相关设置未开启主机名校验，或存在弱校验情况。 未见异常：相关设置对主机名进行强校验或使用了 CA 机构签发的证书。

编号	数据交互风险-5
测评项目	随机数不安全使用
风险描述	随机数生成机制设置不当可能导致生成的随机数可被预测，威胁密钥安全性。
标准要求	5.3 e）
测评方法	反编译样品文件，查验是否使用不安全的随机数方法。
测评结果	存在风险：发现不安全的随机数方法。 未见异常：未发现不安全的随机数方法。

编号	数据交互风险-6
测评项目	加密算法不安全使用
风险等级	低
风险描述	对称加密算法相关设置不当可能导致加密失效，导致加密文件遭破解、传输数据遭截获等。
标准要求	5.3 e）
测评方法	反编译样品文件，查验是否使用了不安全的 AES/DES 加密算法。
测评结果	存在风险：发现使用不安全的加密算法（如 RC4、AES ECB 或 OFB 工作模式等）。 未见异常：未发现使用不安全的加密算法（如 RC4、AES ECB 或 OFB 工作模式等）。

6.4 重要组件安全测评

编号	组件安全-1
测评项目	系统组件不安全配置
风险描述	系统组件策略、规则不安全配置可能导致相关组件遭恶意调用，为恶意行为提供便利。
标准要求	5.4 a)
测评方法	反编译样品文件，查验组件调用过滤规则、调用路径是否存在不安全配置。

测评结果	存在风险：发现组件调用过滤规则、调用路径存在不安全配置。 未见异常：未发现组件调用过滤规则、调用路径存在不安全配置。。

编号	组件安全-2
测评项目	WebView 组件不安全配置
风险描述	WebView 组件加载网页、功能、资源时，如果存在不安全配置，可能导致数据泄露、劫持、篡改等风险。
标准要求	5.4 c)d)
测评方法	反编译样品文件，查验 WebView 相关功能是否存在不安全配置。
测评结果	存在风险：发现 WebView 相关功能存在不安全配置。 未见异常：未发现 WebView 相关功能存在不安全配置。

编号	组件安全-3
测评项目	Intent 越权调用
风险描述	Intent 组件调用未进行严格过滤，可能导致构造特殊格式的 URL 越权调用 Activity 组件。
标准要求	5.4 e)
测评方法	反编译样本文件，查验 Intent 调用是否进行的严格过滤。
测评结果	存在风险：存在 Intent 组件调用，且未设置过滤策略。 未见异常：未进行 Intent 组件调用或设置了过滤策略。

编号	组件安全-4
测评项目	Intent 隐式调用漏洞
风险描述	使用隐式 Intent 调用时，并未对消息接收方进行限制，可能导致 Intent 内容泄露。
标准要求	5.4 e)
测评方法	反编译样本文件，查验是否隐式调用 Intent 函数。
测评结果	存在风险：使用了隐式调用 Intent 函数方法。 未见异常：未使用了隐式调用 Intent 函数方法。

编号	组件安全-5
测评项目	应用本地拒绝服务漏洞
风险描述	如调用 Intent 函数时未校验输入参数，如存在异常输入，可能导致崩溃。
标准要求	5.4 f)
测评方法	对 Intent 导出的组件传递一个不存在的序列化对象，查验是否导致程序进程崩溃。
测评结果	存在风险：程序进程崩溃。 未见异常：程序进程未崩溃。

6.5 代码及资源文件安全测评

编号	代码及资源文件安全-1
测评项目	代码未混淆/加固
风险描述	代码未进行混淆或加固可能降低反编译难度，易暴露代码逻辑，导致安全机制遭绕过、

	破解等风险。
标准要求	5.5 a)
测评方法	反编译文件，查验代码关键类名、逻辑、赋值等是否进行混淆处理。
测评结果	存在风险：代码未混淆处理。 未见异常：代码已混淆处理。

编号	代码及资源文件安全-2
测评项目	SO 文件未混淆/加固
风险描述	SO 文件包含的动态链接库文件，未混淆/加固可能导致代码运行逻辑等信息泄露。
标准要求	5.5 b)
测评方法	反编译样品文件，静态扫描代码文件，查看样品文件是否对 SO 文件进行混淆加固。
测评结果	存在风险：扫描反编译后的代码文件，发现样品中的 SO 文件未进行加固。 未见异常：扫描反编译后的代码文件，发现样品中的 SO 文件已进行加固。

编号	代码及资源文件安全-3
测评项目	H5 资源文件未加密
风险描述	明文存储的 H5 资源文件可能遭篡改，导致非法植入页面、恶意代码等安全风险。
标准要求	5.5 c)
测评方法	反编译样品文件，查验是否存在明文存储的 H5 文件。
测评结果	存在风险：发现存在明文存储的 H5 文件。 未见异常：未发现存在明文存储的 H5 文件。

编号	代码及资源文件安全-4
测评项目	未限制解压文件名
风险描述	热更新禁止未限制解压文件名可能导致文件被解压至任意路径，导致恶意文件覆盖正常文件。
标准要求	5.5 d)
测评方法	反编译样品文件，查验是否使用 ZipArchive 实现解压功能且允许任意压缩文件名。
测评结果	存在风险：发现使用 ZipArchive 实现解压功能且允许任意压缩文件名。 未见异常：未发现使用 ZipArchive 实现解压功能且允许任意压缩文件名。

编号	代码及资源文件安全-5
测评项目	动态加载 Dex 文件篡改
风险描述	热更新机制允许动态加载 Dex 文件且未限制 Dex 编辑，可能导致目标文件被篡改。
标准要求	5.5 d)
测评方法	反编译样品文件，查验是否允许动态加载 Dex 文件，如是，则检查 Dex 文件是否可修改。
测评结果	存在风险：允许动态加载 Dex 文件且 Dex 文件可读写。 未见异常：未允动态加载 Dex 文件或 Dex 文件不可读写。

编号	代码及资源文件安全-6

测评项目	未使用编译器堆栈保护技术
风险描述	向内存缓冲区内填充数据位数超过缓冲区本身的容量，可能导致溢出的数据覆盖在合法数据上，呆滞内存中将执行的程序地址被修改。
标准要求	5.5 e)
测评方法	反编译样品文件，查验 so 文件是否使用了编译器堆栈保护技术。
测评结果	存在风险：发现使用了编译器堆栈保护技术。 未见异常：未发现使用编译器堆栈保护技术。

编号	代码及资源文件安全-7
测评项目	未使用地址空间随机化技术
风险描述	如应用程序的地址空间布局固定，其区域的基地址可能被获取，导致注入代码被执行。
标准要求	5.5 f)
测评方法	反编译样品文件，查验 so 文件是否使用了地址空间随机化技术。
测评结果	存在风险：发现使用了地址空间随机化技术。 未见异常：未发现使用地址空间随机化技术。

编号	代码及资源文件安全-8
测评项目	密钥明文硬编码
风险描述	代码内存在密钥信息硬编码，可能导致鉴权信息泄露、加密流量遭破解。
标准要求	5.5 g)
测评方法	反编译样品文件，查验代码内加密函数、方法是否存在明文的硬编码密钥信息。
测评结果	存在风险：未发现明文的密钥硬编码。 未见异常：发现明文的密钥硬编码。

编号	代码及资源文件安全-9
测评项目	URL 信息硬编码
风险描述	代码内存在 URL 明文信息，可能导致后端服务器域名、接口等信息暴露。
标准要求	5.5 h)
测评方法	反编译样品文件，查验代码内是否存在明文 URL 地址信息。
测评结果	存在风险：发现明文的 URL 字符串地址信息。 未见异常：未发现明文的 URL 字符串地址信息。

附 录 A
（资料性）
移动互联网应用程序 SDK 典型安全风险

表A.1给出了SDK典型安全风险的示例。

表A.1 移动互联网应用程序SDK典型安全风险

序号	类型	名称
1	基本安全	SDK 分发缺少完整性校验
2		内含恶意程序
3		调试日志输出敏感信息
4		残留测试信息
5		内嵌无关插件、SDK
6		索要非必要权限
1	数据存储安全	个人信息明文存储
2		数据证书明文存储
3		数据全局可读写
1	数据交互安全	敏感信息 HTTP 协议传输
2		敏感信息明文传输
3		HTTPS 未开启双向认证
4		HTTPS 未验证主机名
5		随机数不安全使用
6		加密算法不安全使用
1	重要组件安全	系统组件属性不安全配置
2		WebView 组件不安全配置
3		Intent 解析协议越权漏洞
4		Intent 隐式调用漏洞
5		本地拒绝服务漏洞
1	代码及资源文件安全	代码未混淆/加固
2		SO 文件未混淆/加固
3		H5 资源文件未加密
4		未限制解压文件名
5		未使用编译器堆栈保护技术
6		未使用地址空间随机化技术
7		动态加载 Dex 文件风险
8		URL 信息硬编码
9		密钥硬编码风险