ICS 03.060
CCS A 11

团 体 标 准

T/NIFA 33-2025

移动金融小程序安全要求

Security requirements for financial mobile mini program

2025-9-10 发布 2025-9-10 实施

中国互联网金融协会 发布

目 次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语与定义 1
4 缩略语 3
5 L1 与 L2 类别要求 3
6 安全要求 3
6.1 身份认证安全 3
6.2 逻辑安全 5
6.3 服务端接口安全 5
6.4 抗攻击能力 6
6.5 密码应用安全 6
6.6 数据安全 7
7 个人信息收集合规要求 9
7.1 收集个人信息告知同意 9
7.2 申请授权 9
7.3 收集行为要求 10
7.4 拒绝或撤回同意要求 10
7.5 更正、删除及注销要求 10
7.6 个人信息处理规则要求 10
8 开发管理要求 10
8.1 代码质量 10
8.2 代码管理 11
8.3 测试验证与交付 11
8.4 文档管理 11
附录 A（规范性）安全类别对应的要求 12
附录 B（资料性）小程序技术架构示意 13
附录 C（资料性）其他类型敏感信息示例 14
参考文献 15

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》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专利的责任。

本文件由中国互联网金融协会提出。

本文件由中国互联网金融协会归口。

本文件起草单位：中国互联网金融协会、中国邮政储蓄银行股份有限公司、深圳前海微众银行股份有限公司、浙江网商银行股份有限公司、蚂蚁科技集团股份有限公司、深圳市腾讯计算机系统有限公司、北京国家金融科技认证中心有限公司、中互金认证有限公司、北银金融科技有限责任公司。

本文件主要起草人：马超、高明、杨彬、单剑锋、于圆、任家琪、田然、曹中全、张建强、孙丹丹、江嘉航、陆碧波、熊伊婧、黄伟斌、蒋增增、张健、史汝辉、李士通、张毅。

移动金融小程序安全要求

1 范围

本文件给出了移动金融小程序的定义，明确了移动金融小程序在安全、个人信息收集、开发管理等方面的要求。

本文件适用于金融机构对移动金融小程序的开发、测试等方面的管理，也适用于评估机构开展移动金融小程序的安全评估。其他机构开发具有金融服务功能的小程序时也可参考本文件。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 35273—2020 信息安全技术 个人信息安全规范

GB/T 44588—2024 数据安全技术 互联网平台及产品服务个人信息处理规则

3 术语与定义

GB/T 35273—2020和JR/T 0171—2020界定的以及下列术语和定义适用于本文件。

3.1

移动金融服务 mobile financial service

金融机构通过移动终端提供的在线金融服务。

注：在线金融服务通常包括账户管理、投资与理财服务、支付与转账服务、信贷与信用服务、信用卡服务、保险服务等。

[来源：ISO 12812—1:2017，3.25，有修改]

3.2

框架型应用软件 frame-based application software

为在移动智能终端上运行，提供数据访问控制和小程序分发等管理能力，并为在其上运行的第三方小程序提供相应开发接口的应用软件。

3.3

小程序 mini program

基于框架型应用软件开放接口实现的，用户无需安装即可使用的移动互联网应用程序。

注：关于小程序的技术架构参考见附录B。

[来源：GB/T 42582—2023，3.7，有修改]

3.4

移动金融小程序 financial mobile mini program

为用户提供移动金融服务的小程序。

3.5

个人金融信息 personal financial information

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

注：个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

[来源：JR/T 0171—2020，3.2]

3.6

C2 类别个人金融信息 personal financial information（C2）

C2 类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害。

[来源：JR/T 0171—2020，4.2]

3.7

C3 类别个人金融信息 personal financial information（C3）

C3 类别个人金融信息为敏感级别最高的个人金融信息，主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害。

注：C3 类别个人金融信息包括但不限于银行卡磁道数据（或芯片等效信息）、卡片验证码（CVN 和 CVN2）、卡片有效期、银行卡密码、网络支付交易密码；账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码；用于用户鉴别的个人生物识别信息。

[来源：JR/T 0171—2020，4.2]

3.8

支付敏感信息 payment sensitive information

支付信息中涉及支付主体隐私和身份识别的重要信息。

注：支付敏感信息包括但不限于银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等用于支付鉴权的个人金融信息。

[来源：JR/T 0171—2020，3.3]

3.9

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注：敏感个人信息包括生物特征、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满14周岁未成年人的个人信息。

[来源：GB/T44588—2024，3.4]

3.10

个人生物识别信息 personal biometric information

个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

[来源：GB/T 35273—2020，5.4]

3.11

敏感信息 sensitive information

敏感信息包括支付敏感信息、敏感个人信息，以及一旦泄露可能会对小程序开发者的业务、合作伙伴和用户带来利益损害的其他类型敏感信息。

注：其他类型敏感信息示例参考附录C。

3.12

授权 authorization

框架型应用软件为小程序提供的申请数据或资源的一种方式。范围涵盖框架型应用所存储的数据或资源及其从操作系统中获取到的数据或资源。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

CRLF：注入回车换行符(Carriage Return Line Feed)

CSRF：跨站请求伪造（Cross Site Request Forgery）

SDK：软件开发工具包（Software Development Kit）

SSRF：服务端请求伪造(Server Side Request Forgery)

TLS：安全传输层协议（Transport Layer Security）

XSS：跨站脚本（Cross Site Scripting）

5 L1与L2类别要求

本文件根据移动金融小程序涉及的服务场景，提出L1、L2两个安全类别的要求，不同类别对应的要求参考附录A，具体适用范围如下：

包含独立评价组的需方组织应履行下列职责：

a) L1要求适用于开展各类型服务的移动金融小程序；

b) L2要求适用于处理C3类别个人金融信息及支付、转账等资金交易场景。

6 安全要求

6.1 身份认证安全

6.1.1 认证信息安全输入

小程序输入用户身份认证信息时要求如下：

输入用户登录密码、银行卡支付密码和网络支付交易密码等用户身份认证信息应采用逐字符掩码、逐字符加密、字符加密、防范键盘窃听、自定义软键盘等防护措施，或其他经攻击测试无法获取认证信息明文的安全防护措施。（L2）

框架型应用软件宜通过API或端原生功能等形式，为小程序提供安全键盘。

6.1.2 用户认证方式

小程序开展用户身份认证时要求如下：

a) 登录时利用小程序平台提供的用户唯一标识识别用户身份，并建立账号绑定关系的应符合小程序平台相关要求；
b) 登录态进行敏感操作时应对用户进行身份认证，例如，发生支付、转账、购买理财等资金交易时满足相关业务管理要求对用户身份进行认证；
c) 当使用独立于小程序平台的身份认证时，应使用密码、短信验证码、手势密码、生物特征识别等用户身份认证方式，不应仅使用手机号码、身份证号码等作为认证要素；
d) 当小程序与机构自有 APP 应用共用账户体系时，小程序端的登录及转账、支付、理财等资金交易身份认证要求不应低于自有 APP 应用；（L2）
e) 应建立唯一的、具有一定复杂度的用户会话标识标记登录态，禁止使用固定会话标识；
f) 使用短信验证码作为身份验证要素时，短信验证码应仅可成功使用一次，且具有有效期、长度和随机性的要求；具有验证错误次数限制，不应超过 3 次；具有获取时间限制，在规定时间内获取次数不能超过限定的最大次数；短信验证码所在的短信内容中，应告知用户短信验证码的发送方、用途以及有效时间，并提示请勿将验证码告知他人，泄露将影响账户安全；
g) 图形验证码具有使用时间限制并仅能使用一次，图形验证码由服务器生成，小程序客户端源文件中不包含图形验证码文本内容。图形验证码不应单独作为身份验证通过要素；
h) 短信验证码长度不少于 6 位，有效期不长于 6 分钟；（L2）
i) 登录态进行涉及如大额资金交易或同等敏感操作时采用了两种或两种以上要素对用户身份进行认证。（L2）

注：本条款关注点是对于敏感操作应设置的身份认证策略，在标准应用中机构应根据监管要求、业务风险情况明确敏感操作范围。机构应具有大额资金交易范围的定义，大额资金交易不包括购买基金或理财产品等场景下的资金交易。

6.1.3 认证失败处理

小程序进行用户身份认证失败时要求如下：

a) 应具有合理的认证失败处理功能，如采取结束会话、限制失败认证次数、账户暂时锁定和自动退出等措施，控制措施应在服务端实现；
b) 认证失败时，应模糊错误提示信息，错误提示信息不应泄露用户账号、交易金额等敏感个人信息。

6.1.4 密码设定与重置

当小程序支持密码设定与重置时，要求如下：

a) 若设置基于小程序独立的登录密码，密码复杂度满足以下两种要求之一：
   1) 长度至少8位且至少包含数字、大写字母、小写字母以及特殊字符中的两种或两种以上组合；
   2) 具有有效抵御彩虹表等密码破解攻击的防护措施，登录密码至少6位，具有一定的复杂度要求，不可设置简单密码，如连续数字、键盘上相邻按键的字符、网络应用或设备的默认口令等。
b) 若设置交易密码，不应设置简单密码（如“111111”、“123456”）或与用户个人信息（如出生日期、证件号码、手机号码）相似度过高的密码；
c) 若设置初始密码，初始密码应随机生成，应强制用户在首次登录后修改初始密码；
d) 修改密码时应验证当前有效密码，验证时应对密码输入错误次数进行限制，最大不宜超过 5 次；
e) 修改密码时新密码不可与当前有效密码相同；

f） 密码重置时，应使用短信验证码、用户注册信息验证等方式，对用户身份进行校验。宜采用双因素身份认证方式，对用户身份进行校验。

6.2 逻辑安全

6.2.1 业务逻辑设计

小程序在业务逻辑设计时要求如下：

a） 重要业务逻辑应放在服务端实现，例如用户身份验证逻辑、认证失败处理措施应在服务端执行，防止攻击者绕过本地控制措施；

b） 对于登录、登出、交易处理、用户身份认证等流程设计应充分考虑其合理性，避免逻辑漏洞的出现，确保认证流程无法被重放和绕过。

6.2.2 风险控制

小程序在登录和交易时风险控制要求如下：

a） 应设置合理的登录风险控制策略，包括但不限于：

1） 当用户闲置在线状态超出时限时，采取合理的账户登录超时控制策略；

2） 合理的多点登录策略，如提示登录信息或退出先登录的账户等策略。

b） 当具有资金交易功能时应采取合理的交易风险控制策略，包括但不限于：

1） 针对不同的资金交易金额，应设计合理的身份认证策略，如对于大额交易，实施多因素验证或额外的安全措施；

2） 针对不同的资金交易业务场景，采取了合理的策略，如限额控制策略、时限控制策略、异常交易冻结策略等。

6.2.3 异常处理

小程序在异常处理时要求如下：

a） 发生运行故障时产生的异常信息，不应泄露用户的敏感个人信息；

b） 当交易出现异常时，应向客户提示出错等信息，但不应泄露用户的敏感个人信息。

6.3 服务端接口安全

小程序服务端接口安全要求如下：

a） 服务端对外提供的 API 应采用鉴权机制（如 OAuth 2.0），验证调用者的身份和权限；敏感信息、能力相关接口应在后台进行鉴权，例如校验 openid、IP 地址、自定义登录态等信息。鉴权逻辑应放在后台进行，不应在小程序前端以隐藏页面、隐藏按钮等方式来代替，接口鉴权要求包括：

1） 应避免水平越权攻击。服务端与小程序交互的数据接口，应对用户的身份（如Cookies、authcode、AccessToken、前置操作等）进行充分鉴权，不能只依赖于传入参数，防止攻击者伪装成他人发起请求；

2） 应避免垂直越权攻击。服务端与小程序交互的数据接口，应在服务端对用户权限进行校验。

b） 服务端接口应对请求的参数、富文本进行有效过滤，防止通过非法输入特殊字符和命令，进行 XSS 攻击、SQL 注入、命令注入等常见 web 攻击；

c） 服务端应对用户请求操作的合法性进行判断，包括但不限于：

1） 应判断请求的来源是否是自己域名或合作服务方，防止用户被CSRF攻击，导致攻击者直接获得用户的敏感操作权限；

2） 应对用户的权限及前置操作进行验证，防止用户绕过验证逻辑；
3） 对于返回重要数据或完成重要操作的请求，如登录，应增加一次性凭证，防止攻击者劫持到用户登录凭证，重放攻击从而获得权限。

d） 应对接口请求设置合理的频率限制，防止暴力破解和 DDoS 攻击；
e） 应从服务端对对上传文件类型、格式等做合法性校验。应判断并限制上传文件的类型，防止攻击者上传恶意代码。文件存储时，应设置文件存储权限为只读，不可执行，并与系统其它重要代码、数据隔离；
f） 应正确限制可下载文件所在的目录范围，应检查用户下载权限，下载的文件需与其它重要数据、文件、代码隔离，管控访问路径，防止攻击者读取到其它目录下的重要数据；
g） 应对请求的参数及时间进行签名，防止攻击者伪造请求数据。（L2）

6.4 抗攻击能力

6.4.1 防逆向与静态分析

小程序在防逆向与静态分析方面，对小程序前端代码应进行必要的加固保护，可采用代码加密、压缩、混淆、反调试等加固措施之一或组合，核心代码应进行全面加固。

6.4.2 防动态分析

小程序在防动态分析方面要求如下：
a） 应通过数据加密等方式，防止网络流量的动态分析；
b） 应具有防止网络通信过程中重放攻击、中间人攻击的能力。

框架型应用软件宜提供以下能力：
a） 具有检测和防御逆向工程工具与框架的机制；
b） 具有防止中间人攻击的能力。

6.4.3 防已知漏洞

小程序在已知漏洞防范方面要求如下：
a） 应具有源代码暴露、应用已知脆弱性的组件、SQL 注入、XSS 攻击、CSRF、CRLF 注入、SSRF、代码注入、命令注入以及任意文件上传、任意文件下载等已知漏洞的防范能力；
b） 当小程序使用 webview 相关组件时，应仅加载预定义的安全域名列表中的 H5 网页链接，从而防止攻击者利用 webview 相关组件加载恶意 H5 链接。

框架型应用软件提供webview相关组件时，应配套提供域名管控功能，以限制webview相关组件加载的H5网页链接的域名范围。

6.5 密码应用安全

6.5.1 密码算法

小程序在使用密码算法方面要求如下：
a） 应使用框架型应用软件提供的加密 API 或不存在已知漏洞的算法库；
b） 不应使用已知的弱密码算法，例如:DES、RC2、RC4、BLOWFISH、MD4、MD5、SHA1 等；
c） 应使用符合行业最佳实践的密码算法配置，避免出现以下常见配置问题：
1） 密钥长度不足，例如RSA密钥长度小于2048；
2） 使用对称加密算法时选择安全性低的分组模式，例如ECB模式；

3) 使用硬编码的密钥加密本地存储的数据，硬编码的密钥指密钥是应用程序资源的一部分、可从已知值中得出的值或代码中硬编码；
4) 使用弱随机数发生器；
5) 使用自定义加密算法。

框架型应用软件宜提供安全的加密算法API、随机数生成API。

6.5.2 密钥管理

小程序在密钥管理方面要求如下：

a) 应确保密钥生成的随机性和不可预测性，不应出现弱密钥生成功能，例如不得直接使用用户提供的密码作为密钥；
b) 应保护存储中的密钥，使用密钥加密密钥来加密数据加密密钥；
c) 应保护内存中的密钥，确保密钥在内存中存活的时间尽可能短，并加密操作成功后，以及在出现错误的情况下，清除内存中密钥；
d) 应保护传输中的密钥，使用安全的传输协议，并将密钥进行加密后传输，使用 MAC 或数字签名等措施，确保密钥在传输过程中的机密性和完整性。

框架型应用软件宜提供密钥管理API，提供密钥生成、存储等功能。

6.6 数据安全

6.6.1 数据获取-数据防窃取

小程序在数据防窃取方面要求如下：

a) 敏感信息（例如 AppSecret、AccessKey 及其他敏感的配置信息）不应以明文、注释、可逆的编码方式（如 base64）、不安全散列函数（如 MD5、SHA1）等形式出现在小程序文件内；
b) 临时文件中不应出现支付敏感信息，临时文件包括但不限于 Cookies、本地临时文件等；
c) 本地日志数据不应包含支付敏感信息，不应包含完整的敏感信息原文；
d) 敏感信息脱敏的逻辑，应在服务端完成，不能在小程序客户端进行脱敏，同时代码注释、隐藏域、URL 参数、Cookies 中的数据，也应脱敏；
e) 服务端应禁止返回明文敏感信息；
f) 对于内存中 C3 类个人金融信息(例如登录密码、支付敏感信息等)的保护，应确保该类信息由尽可能少的组件处理，确保当包含该类信息的对象不再需要时，正确地删除对象引用，确保该类信息一旦不再需要就被覆盖；（L2）
g) 应实现身份认证过程的防截屏、录屏，如输入手势验证码、登录密码、支付密码等；(L2)
h) 运行时内存中不存在登录密码、完整的银行卡密码和网络支付交易密码明文。（L2）

框架型应用软件应提供防截屏、录屏API，宜提供内存数据清理功能。

6.6.2 数据获取-数据有效性

小程序在数据有效性方面要求如下：

a) 在数据获取时提供有效性校验功能，确保通过人机接口或通信接口输入的数据格式或长度等信息符合系统设定要求；
b) 对用户输入的特殊字符进行严格过滤，如’、″、<、>、/、*、；、+、-，&、|、(、)、and、or、select、union 等，或采用预编译，固定语法结构和绑定变量等非过滤器方式保证输入内容安全，防止 SQL 注入。

6.6.3 数据访问控制

框架型应用软件应为小程序提供文件存储及运行时隔离环境，保证其他小程序及框架型应用软件本身不能非法访问目标小程序。

6.6.4 数据传输-网络通信安全

小程序在网络通信方面要求如下：

a) 应与服务器之间建立安全的信息传输通道，例如使用 TLS V1.2 或 TLS V1.3；
b) 小程序服务端安全协议版本应及时更新至安全稳定版本，确保采用的安全协议不包含已知的公开漏洞，使用业界推荐的 TLS 密码套件；
c) 小程序应仅与指定的域名进行网络通信。

框架型应用软件宜为小程序提供安全的网络传输能力，例如使用TLS V1.2或TLS V1.3，确保采用的安全协议不包含已知的公开漏洞，使用业界推荐的TLS密码套件。

6.6.5 数据传输-数据保密性与完整性

小程序在数据传输过程中保密与完整性要求如下：

a) C3 类个人金融信息，例如登录密码、支付敏感信息等，在通过公共网络传输时，除了满足网络通信安全要求外，还应采取数据加密等措施确保其保密性；
b) 关键的交易数据、个人身份信息、业务数据等，如收款人信息、交易金额、订单号等（C2/C3 类个人金融信息数据），在通过公共网络传输时，除了满足网络通信安全要求外，应采取措施（如数字签名、MAC 等）确保其完整性。

6.6.6 数据存储

小程序的客户端在数据存储方面要求如下：

a) 不应明文保存用户敏感信息，例如对称密钥、私钥等密钥信息，手机号、身份证号等敏感信息；
b) 不应以任何形式存储支付敏感信息及个人生物识别信息的样本数据、模板。

6.6.7 数据展示

小程序在数据展示方面要求如下：

a) 登录、支付等口令框应默认屏蔽展示，且屏蔽展示时使用同一特殊字符代替；
b) 不应明文显示登录密码、银行卡密码、网络支付交易密码等用户鉴别类信息；
c) 处于未登录状态时，不应展示与个人信息主体相关的 C3 类别个人金融信息；
d) 除交易对账、转账收款方确认等必须由用户确认的情况外，对于银行卡号、手机号码、证件类识别标识或其他识别标识信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证；
e) 涉及其他信息主体的信息时，应对显示的信息进行屏蔽展示，当满足如下条件之一时可不脱敏：
   1) 其他方主动发起的活动包含的信息，如其他方发起交易、收付款；
   2) 与其他方已建立信任关系(间接授权)，如向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人；
   3) 其他法律法规要求的情况。

6.6.8 数据销毁

小程序客户端在数据销毁方面要求如下：

a) 残余信息保护方面，账户退出时应清除非业务功能运行所必需留存的业务数据，保证用户信息的安全性；

b) 页面返回保护方面，应支持页面返回后自动清除银行卡密码、网络支付交易密码、登录密码等敏感信息的机制；
c) 会话失效方面，退出登录时应向服务器发送会话结束请求，使当前会话状态失效。

7 个人信息收集合规要求

7.1 收集个人信息告知同意

小程序收集个人信息的告知同意要求如下：

a) 收集个人信息前应向用户告知并获得授权同意或具备其他合法性基础，告知方式包括但不限于征求用户同意个人信息处理规则、授权弹窗等，在首次启动页面上应展示个人信息处理规则；
b) 个人信息处理规则应简洁、清晰描述其收集个人信息的目的、方式及范围，应当突出显示敏感个人信息的处理目的、方式和范围；
c) 小程序向用户征求收集个人信息的同意环节，应提供明确的同意或拒绝选项，不应仅使用“好的”、“我知道了”等无法清晰表达用户同意的词语，不应设置为默认同意或采用默认勾选、缩小文字、冗长文本等方式诱导用户同意个人信息处理规则；
d) 小程序应将个人信息处理规则访问入口放置在功能菜单的明显入口，访问路径不超过 4 层，用户在登录或未登录状态下应均可访问查阅；
e) 以用户同意为小程序处理个人信息合法性基础的，当个人信息处理的目的、方式、范围发生变更时，应重新告知用户并征得用户同意；
f) 收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，且描述应明确具体、通俗易懂，并征得个人信息主体的明示同意；
g) 收集不满 14 周岁未成年人个人信息，应制定专门的个人信息处理规则，并取得未成年人监护人的单独同意。

注：关于个人信息处理规则的要求适用于与框架型应用软件不属于同一主体的第三方小程序。

7.2 申请授权

小程序申请授权应满足以下要求：

a) 小程序申请授权时，应同步告知申请使用的目的，目的应明确具体且易于理解，不包含任何欺诈、诱骗、误导用户授权的描述；
b) 小程序申请授权时，应在使用对应业务功能时提出申请，不应提前向用户弹窗申请授权，不应以捆绑方式要求用户一次性同意多个授权，不得默认、捆绑或使用其他手段变相欺骗、误导、强迫个人信息主体授予权限；
c) 小程序申请授权应为实现业务功能所必需，应与提供的业务功能或服务具备合理的相关性；
d) 小程序应提供便捷、有效、完整的授权撤销渠道；
e) 未经用户同意，不应随意更改用户的授权状态；
f) 小程序不应发生以下违规申请授权的行为：
    1) 拒绝授权小程序强制退出或关闭：小程序运行时，向用户申请授权，用户拒绝授权后，小程序退出或关闭，或拒绝提供与申请授权无关的功能服务；
    2) 拒绝授权小程序弹窗循环：小程序运行时，向用户申请授权，若用户拒绝授权后，小程序循环弹窗申请授权，使用户无法继续使用；
    3) 频繁申请授权：小程序运行时,用户拒绝授权后，在非业务场景所必需或在非用户主动触发授权所涉及的业务场景的情况下，再次弹出与当前服务场景无关的授权弹窗即为频繁，

例如拒绝授权后，用户重新打开小程序或切换小程序不同页面时，向用户申请开启与当前服务场景无关的授权，影响用户正常使用。

框架型应用软件宜为小程序申请授权提供同步告知、授权撤销的功能。

7.3 收集行为要求

小程序收集个人信息时应满足以下要求：

a） 未经用户同意或未取得处理个人信息的其他合法性基础，不得收集个人信息；

b） 收集的个人信息范围应与告知用户的范围一致，仅在客户端处理就可实现相关功能的，不应将个人信息回传至后台服务器；

c） 应仅在用户使用业务功能期间,收集该业务功能所需的个人信息;小程序处于静默、后台运行、退出等状态，且未向用户提供服务时，不应收集用户个人信息；

d） 不应通过积分、奖励、优惠、红包等方式，欺骗误导用户提供与小程序业务功能无关的个人信息或授权；

e） 不应仅以服务体验、产品研发、算法推荐、风险控制等为由，强制要求用户同意超范围或者与服务场景无关的个人信息收集行为；

f） 收集个人信息的频度不超出业务功能实际需要。

7.4 拒绝或撤回同意要求

基于用户同意处理个人信息的，当用户拒绝或撤回同意时，应满足以下要求：

a） 应保证与拒绝或撤回个人信息收集、授权无关的业务功能正常使用；

b） 不应强制退出或关闭小程序，法律法规另有规定的除外。

7.5 更正、删除及注销要求

基于用户同意处理个人信息的，应满足以下要求：

a） 应提供有效的更正、删除个人信息及注销用户账号功能，且不应设置不必要或不合理条件；

b） 应及时响应用户请求，需人工处理的，应在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理，宜在 15 日内完成处理。

7.6 个人信息处理规则要求

小程序提供的个人信息处理规则内容应满足GB/T 35273—2020第5.5（a）节要求。宜满足GB/T 44588—2024第8.1节、8.3节、8.4.1 b）条、8.4.1 i）条、8.4.2节、8.4.3节的要求。

8 开发管理要求

8.1 代码质量

小程序的代码质量要求如下：

a） 正式发布前，应关闭小程序调试模式，关闭测试接口调用，防止信息泄露；

b） 按照 6.4.1 要求对小程序前端代码进行必要的加固；

c） 上线前执行安全漏洞扫描，对于新建、日常变更等不同阶段可执行不同的扫描策略；

d） 审核并记录引入的第三方组件，使用第三方 SDK 或服务时，要对其进行安全审核，确保它们不会引入安全风险；

e） 针对服务端接口、业务逻辑、加密及数据安全等方面定期进行渗透测试；

f） 针对漏洞扫描、渗透测试等安全测试中发现的高风险问题应及时处理，不能及时处理的问题应

进行安全影响分析。

8.2 代码管理

小程序的代码管理要求如下：

a) 制定安全编码规范，并在开发过程中严格执行；
b) 编码完成后使用代码扫描工具和人工代码检查方式进行评审，识别安全缺陷并修复；
c) 对源代码的访问进行权限控制，在小程序代码管理平台等源码管理工具内配置适当的访问权限；
d) 对源码库进行修改、更新或发布等操作时需要经过授权和批准；
e) 应使用 SVN/GIT 等配置管理工具管理源码，保证源码的变更均可被记录、追溯；
f) 正式生产发布的源码版本在配置管理工具中应被明显标记，以便追溯；
g) 当代码由供应商提供时，编码完成后将代码回收并防止泄密；
h) 应防止备份文件和版本管理工具产生的目录或文件被带到生产环境，避免可能发生的源码泄漏。

8.3 测试验证与交付

测试及交付要求如下：

a) 应建立安全测试机制，提出安全需求，并编制相应的安全测试用例，描述安全测试方法，执行安全测试；应根据变更情况建立安全检测与隐私合规测试的执行策略；
b) 在小程序新建时应执行全面的安全测试与隐私合规测试，形成测试总结报告；
c) 应将测试环境与系统开发环境、生产环境隔离，不应使用生产环境作为测试环境，不应将测试环境转为生产环境；
d) 应建立小程序交付验收流程和制度，并在新建、升级和更新版本时进行交付验收。

8.4 文档管理

小程序开发过程中，对开发生命周期各阶段的产出的文档（如需求说明书、安全设计方案、测试设计文档、测试用例、测试总结报告等）进行配置管理、归档并设置相应访问权限。

附 录 A
（规范性）
安全类别对应的要求

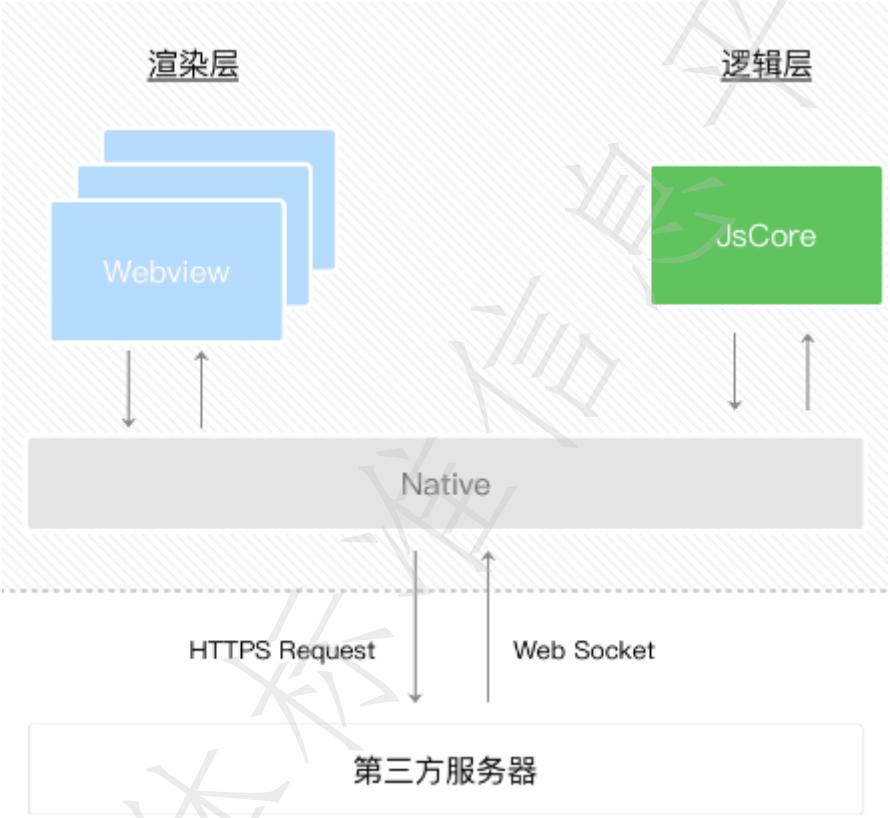
本文件各条款要求所属的安全类别见表A.1。（其中●表示该类别的安全要求、○表示非该类别的安全要求）

表A.1 L1/L2 安全类别对应的安全要求

章节编号	L1	L2
6.1.1	○	●
6.1.2(a)-(c)	●	○
6.1.2(d)	○	●
6.1.2(e)-(g)	●	○
6.1.2(h)-(i)	○	●
6.1.3	●	○
6.1.4	●	○
6.2.1	●	○
6.2.2	●	○
6.2.3	●	○
6.3(a)-(f)	●	○
6.3(g)	○	●
6.4.1	●	○
6.4.2	●	○
6.4.3	●	○
6.5.1	●	○
6.5.2	●	○
6.6.1(a)-(e)	●	○
6.6.1(f)-(h)	○	●
6.6.2	●	○
6.6.4	●	○
6.6.5	●	○
6.6.6	●	○
6.6.7	●	○
6.6.8	●	○
7	●	○
8	●	○

附 录 B
（资料性）
小程序技术架构示意

小程序的技术架构示意如图B.1所示，框架型应用软件给小程序所提供的环境为宿主环境，宿主环境为小程序提供网络通信能力、组件、API。



图B.1 小程序技术架构示意图

小程序的运行环境分成渲染层和逻辑层，渲染层和逻辑层分别由2个线程管理，渲染层的界面使用了webview 相关组件进行渲染；逻辑层采用JsCore线程运行JS脚本。一个小程序存在多个界面，所以渲染层存在多个webview线程，这两个线程的通信会经由框架型应用软件（上图中以Native来代指）做中转，逻辑层发送网络请求也经由Native转发。

附 录 C
（资料性）
其他类型敏感信息示例

其他类型敏感信息示例见表C.1。

表 C.1 其他类型敏感信息示例

类别	典型示例
与框架型应用软件相关的信息	AppSecret、AccessKey
密钥信息	私钥（RSA 私钥、SM2 私钥）、对称密钥（AES 密钥、SM4 密钥）
认证信息	Token、API 凭证、消息推送密钥、第三方服务接入凭证等
日志信息	含用户数据的程序异常信息、调试日志等

参 考 文 献

[1] GB/T 35273—2020 信息安全技术 个人信息安全规范
[2] GB/T 42884—2023 信息安全技术 移动互联网应用程序（App）生命周期安全管理指南
[3] JR/T 0171—2020 个人金融信息保护技术规范
[4] JR/T 0092—2019 移动金融客户端应用软件安全管理规范
[5] T/TAF 180.1—2023 小程序个人信息保护规范 第1部分：申请授权行为
[6] T/TAF 180.2—2023 小程序个人信息保护规范 第2部分：个人信息收集行为
[7] OWASP Mobile Application Security Testing Guide(MASTG) V1.5
[8] OWASP Mobile Application Security Verification Standard (MASVS) v2.0.0