ICS 03.060
CCS A 11

团　　体　　标　　准

T/AMAC 0001—2023

基金管理公司移动互联网应用程序技术规范

Mobile Application Technical Specifications of Asset Management Companies

2023-09-12 发布　　2023-09-12 实施

中国证券投资基金业协会　　发布

目　　次

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》的规定起草。

本文件由中国证券投资基金业协会提出。

本文件由中国证券投资基金业协会归口。

本标准主要起草单位：易方达基金管理有限公司、工银瑞信基金管理有限公司、上海东方证券资产管理有限公司、中国证券投资基金业协会

本标准主要起草人员：陈丽园、唐永鹏、刘硕凌、李明、梅亚雷、杨飞、郭慧峰、谢橦、张化军、张强、许恩泽、许可、张伟、高国钊

基金管理公司移动互联网应用程序技术规范

1 范围

本文件规定了公募基金管理公司移动互联网应用程序在软件安全、用户个人信息安全、兼容性、性能、交互等方面的技术要求和软件研发运维等环节的管理要求。

本文件适用于公募基金管理公司向用户提供金融业务的移动互联网应用程序及其关联的后台服务。

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，注明日期的引用文件，仅该日期对应的版本适用于本文件；不注明日期的引用文件，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 39786—2021 信息安全技术 信息系统密码应用基本要求

JR/T 0060—2021 证券期货业网络安全等级保护基本要求

JR/T 0092—2019 移动金融客户端应用软件安全管理规范

JR/T 0098.3—2012 中国金融移动支付检测规范第3部分：客户端软件

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0192—2020 证券期货业移动互联网应用程序安全规范

JR/T 0240—2021 证券期货业移动互联网应用程序安全检测规范

JR/T 0246—2022 面向老年人的证券期货业移动互联网应用程序设计规范

3 术语与定义

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 applications

通过预装下载等方式，获取并运行在移动智能终端上，用于证券、基金、期货业务查询、交易、业务办理等业务相关的应用程序。

注：移动互联网应用程序包含但不限于业务办理类、证券期货交易类的移动互联网应用程序。

[来源：JR/T 0192—2020，3.2]

3.2

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果。

注：该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的不可

否认性。

[来源：JR/T 0255—2022，3.11]

3.3

代码混淆 obfuscated code

将计算机程序代码转换成功能等价、难以理解的形式。代码混淆可用于程序源代码，也可用于程序编译而成的中间代码。

3.4

重放攻击 replay attacks

重放攻击是攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。

3.5

溢出攻击 buffer overflow attacks

溢出攻击是利用缓冲区溢出漏洞所进行的攻击行动。缓冲区溢出在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可导致程序运行失败、系统关机、重新启动等后果。

3.6

跨站脚本攻击 cross site scripting

跨站脚本攻击（以下简称“XSS”）指利用网站漏洞恶意盗取用户信息。

3.7

SQL 注入 SQL injection

攻击者通过在web应用程序的输入数据中混入SQL片段的方式，绕过应用程序的权限控制机制，直接对数据库进行越权操作，包括但不限于查询、删除、修改、新增未授权数据，对数据库进行破环性操作等。

3.8

身份鉴别 identity authentication

证明一个实体所声称身份的过程。

[来源：JR/T 0255—2022，3.10]

3.9

彩虹表 rainbow table

彩虹表是一个为加密散列函数逆运算而预先计算好的表，用于破解密码的散列值，恢复由有限集字符组成的固定长度的纯文本密码。

3.10

钓鱼攻击 phishing attack

钓鱼攻击是通过给攻击目标发送诱骗性信息,诱导其访问恶意网站,以获取其个人敏感信息,从而实现价值盗取的行为。

3.11

渗透测试 penetration test

通过模拟恶意黑客的攻击方法，来评估计算机网络系统的安全性。

3.12

金融数据 financial information

C1金融数据 C1 financial information

C1类别信息主要为机构内部的信息资产。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响，包括但不限于账户开立时间、开户机构、支付标记信息等。

C2金融数据 C2 financial information

C2类别信息主要为可识别信息主体身份与金融状况的个人金融信息。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，包括但不限于支付账号、证件信息、手机号码、账户登录名、个人财产信息、交易信息等。

C3金融数据 C3 financial information

C3类别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，包括但不限于：银行卡磁道数据卡片有效期、账户登录密码、交易密码、用于用户鉴别的个人生物识别信息等。

[来源：JR/T 0171—2020，4.2，有修改]

4 缩略语

下列缩略语适用于本文件。

XSS	跨站脚本攻击	Cross Site Scripting
IP地址	互联网协议地址	Internet Protocol Address
IPv4	网际协议版本4	Internet Protocol version 4
IPv6	网际协议版本6	Internet Protocol version 6
SQL	结构化查询语言	Structured Query Language
SSL	安全套接层	Secure Sockets Layer
HTTP	超文本传输协议	HyperText Transfer Protocol
HTTPS	超文本传输安全协议	HyperText Transfer Protocol Secure
HTML	超文本标记语言	HyperText Markup Language
URL	统一资源定位符	Uniform Resource Locator
API	应用编程接口	Application Program Interface
SDK	软件开发工具包	Software Development Kit
QPS	每秒请求数	Query Per Second
CPU	中央处理器	Central Processing Unit
OCR	光学字符识别	Optical Character Recognition

5 移动互联网应用程序安全要求

5.1 软件安全

5.1.1 基本安全要求

应满足以下要求：

a）应满足JR/T 0092—2019中的基本要求，宜满足该规范提及的增强要求；应满足JR/T 0192—2020中的各项安全要求；应满足JR/T 0098.3—2012中的各项安全要求；应满足JR/T 0240—2021中的A类检测项和B类检测项要求；

b）应满足JR/T 0060—2021、GB/T 39786—2021中的对应安全等级要求。

5.1.2 网络环境安全

5.1.2.1 通信安全

应满足以下要求：

a）应使用HTTPS协议通信，并使用安全的传输协议（如TLS1.2），避免使用SSL3.0等已被证明存在漏洞的协议；

b）检查用于HTTPS的授权证书，应防止用户在设备上使用自签名的证书进行传输报文的恶意分析。如检测到证书异常，可停止网络通信；

c）使用SSL通信时，应选择符合国家密码主管机构要求的软硬件及算法。

5.1.2.2 抗抵赖

应确保客户端发起的交易类报文的不可抵赖性，对交易相关的客户端特征信息进行留痕，如条件许可，应采用数字证书、时间戳服务器等技术。

5.1.2.3 防重放攻击

对于客户端发起的身份认证或交易报文，服务端应能防止重放攻击。

5.1.3 数据安全

5.1.3.1 数据传输

应满足以下要求：

a） 敏感信息在与本地其他应用软件之间传输时，应采取加密等措施，若本地其他应用软件不能提供相应等级的加密接口，则应评估敏感数据传输的风险，并设计补救措施；

b） 数据在通过公共网络传输时，应采取敏感报文或整体报文加密等措施。

5.1.3.2 数据防窃取

应满足以下要求：

a） 移动互联网应用程序的运行日志中不应打印完整的敏感数据原文；

b） 应支持界面返回后自动清除客户敏感信息的机制；

c） 应防止内存中加密的敏感数据被还原为明文。

5.1.3.3 数据完整性

交易类报文、支付类报文等关键的交易数据，在客户端软件与服务器传输过程中，应采取措施（如：数字签名）以确保其完整性，若本地其他应用不能提供与移动互联网应用程序相应等级的数据完整性保护措施，应评估关键数据传输的风险，并设计补救措施。

5.1.3.4 数据可稽查

客户端应在取得客户授权后，将相关硬件信息留痕到系统中，以便合规稽查。

5.1.3.5 数据有效性

移动互联网应用程序在获取数据时提供有效的校验手段，在通讯报文中，采用随机数、时间戳、交易、令牌等校验技术，保证交易通讯更加安全，防止被篡改和重放攻击。

5.1.3.6 数据防篡改

用户在输入关键交易数据时，如委托代码、交易金额、支付密码等，应采用防篡改机制保证数据不被移动终端的其他程序篡改。

5.1.4 身份鉴权安全

5.1.4.1 安全策略严格分级

对所有的非公开内容访问，应要求身份验证，并严格区分不同权限的可访问内容，不允许用户访问未授权的内容。

5.1.4.2 防登录信息泄露

不应区分登录失败的提示信息（如：用户名不存在、密码错误等），应采用统一的失败提示信息（如：错误的用户名或密码），以避免信息泄露。

5.1.4.3 限定鉴权次数

应满足以下要求：

a） 应限定尝试次数，若尝试过于频繁应锁定用户账户；

b） 同一IP地址或同一终端设备，尝试失败次数过多的，应限制或增强该IP地址或终端设备的身份验证策略，如增加行为验证码。

5.1.4.4 统一鉴权控制

为避免身份验证和访问控制出现遗漏和不一致，应采用集中的方式进行身份验证。如有可能，不同应用可使用SSO等方式进行统一验证。

5.1.4.5 生物特征鉴权

应满足以下要求：

a） 如需开通指纹认证代替口令认证，应完成对用户身份的合法认证；

b） 如用户本地设备的指纹集合发生变更，应重新对用户进行身份认证后才可继续使用指纹认证；

c） 采用人脸识别等其他生物认证方式时，除特定业务外应参考指纹认证的做法；

d） 指纹认证、人脸识别等生物认证技术，不能作为用户身份鉴别的唯一方式；

e） 在处理高风险业务时，指纹认证、人脸识别等生物认证技术应当结合其他身份验证手段，共同完成身份验证。

5.1.4.6 第三方平台鉴权

若首次采用第三方移动互联网应用程序的认证方式，应在该第三方平台鉴权成功跳转回移动互联网应用程序后再次进行口令认证。

5.1.4.7 增强身份认证手段

5.1.4.7.1 基本要求

用户在新设备上初次登录时，应增加短信验证码等增强身份认证手段，进行双因子验证。

对于曾经登录过，但长时间未再次登录的设备，如果用户重新登录，应参考新设备初次登录的场景，进行增强的身份认证手段，建议触发增强身份认证的登录时间跨度阈值不超过90天。

密码重置或其他高风险业务的操作，同样应采取双因子的方式进行身份验证，保证业务安全。

5.1.4.7.2 短信验证码

应满足以下要求：

a） 应确保手机号的真实性得到验证，用户修改手机号应进行严格的身份验证；

b） 短信验证码发送时，应包含相关业务信息，说明短信验证码用途；

c） 应为短信验证码设置合理的有效期；

d） 短信验证码应随机产生，且长度不小于4位；

e） 短信验证码的使用应遵循一码一用的原则，不允许被重复使用，不允许跨业务跨订单使用；

f） 短信验证码短信的内容不应由用户定制；

g） 需要短信验证码的业务场景，应充分论证其业务的必要性，避免造成短信轰炸。

5.1.4.7.3 银行卡鉴权

应满足以下要求：

a） 通过委托银行、银联等国家认可的支付机构完成用户的身份验证；

b） 银行卡鉴权在高风险业务中，一般不能作为唯一验证的手段。

5.1.4.7.4 人脸活体检测技术

应满足以下要求：

a） 应稽核用户与其身份证件的真实性与一致性；

b） 应保护用户的隐私和敏感数据安全；

c） 在高风险业务中，一般不宜作为唯一验证的手段。

5.1.4.7.5 行为验证码

使用行为验证码时，应注意做好容错处理。当验证码服务异常时，不应阻碍相关业务的正常运行。

5.1.5 会话安全

5.1.5.1 使用 SSL 保护会话

应整站使用HTTPS，宜避免在HTTP和HTTPS之间切换。

不应通过HTTP连接传递会话标识。如使用存储用户信息的小型文本文件Cookie（以下简称Cookie），应在授权Cookie上设置安全属性，指示浏览器只通过HTTPS连接向服务器传递Cookie。

5.1.5.2 限制会话有效期

缩短会话有效期可降低会话劫持和会话固定攻击的风险。会话有效期越短，攻击者捕获会话标识并利用它访问应用程序的时间越有限。

客户端与服务器之间的会话有效时长宜为30分钟。

5.1.5.3 服务端管理会话

应在服务端管理会话，不应依赖于客户端对会话的管理，如会话的生成、会话的销毁等都应基于服务器的判断。

5.1.5.4 会话的失效和销毁

应满足以下要求：

a） 用户在登录状态下对账户做敏感操作（如修改密码），应及时在服务器端销毁会话；

b） 用户选择退出登录时，客户端应主动向服务器发送会话结束请求，使会话失效。

5.1.5.5 会话标识安全

应满足以下要求：

a） 会话标识应具有足够的长度和随机性，宜避免出现被猜测的可能性。宜使用30位以上的会话标识，如在会话标识中设计了固定的前后缀，应相应增加标识长度；生成的算法应有足够的随机性，不应仅基于某些要素进行哈希处理；

b） 客户端存储会话标识，应将会话标识存储在安全区域；如存储在浏览器缓存中，应存储在受信任的域名下，设置http-only，宜避免被脚本读取；在移动互联网应用程序中，应存储在受控区域。如存储在内存中，应加密存储，防止使用内存数据存储到磁盘的方式非法获取会话标识。

5.1.5.6 多点登录控制

对于同一个用户在不同平台和终端发起的会话，应控制并发会话数目；不允许同一个账户同时存在多个有效会话，如用户创建了新会话，应使原有会话立即失效。

5.1.5.7 会话数据隔离管理

宜避免将会话数据存储在会话之外，如线程本地存储、缓存、文件、数据库，带来会话管理的风险；如采用池化技术(如对象池、连接池)，宜避免存储会话相关内容，如需存储，应需确保会话结束后清除相关数据。

5.1.6 程序环境安全

5.1.6.1 开发环境安全

开发环境使用的操作系统、数据库、中间件、集成开发环境等系统或软件，应具备安全漏洞管理机制，确保无中高危可利用漏洞。

5.1.6.2 编译安全

生产环境的应用程序包应由专职人员使用专用的编译环境编译生成。编译工具应从官方渠道下载，并对下载后的编译工具进行MD5值校验。

5.1.6.3 运行安全

应满足以下要求：

a）检查应用是否被调试，如被调试，应退出运行或提示用户；

b）检查应用是否运行在模拟器中，如是，应选择退出运行或提示用户；

c）检查设备是否被越狱或根权限破解，如是，应选择退出运行或提示用户；

d）检查系统关键函数（如加密相关的系统函数）是否被劫持，如是，应选择退出运行或提示用户。

如发现上述情况，应告知服务端该设备已被破解，服务端可根据该用户的使用行为，进一步进行安全分级的处理。

5.1.6.4 安装包安全

应满足以下要求：

a）应使用企业证书对移动互联网应用程序进行签名，不发布无数字签名的软件；

b）应对Android程序代码进行代码混淆；

c）应对Android程序进行加固保护；

d）应对iOS安装包内的所有资源进行哈希校验，包括但不限于图片、HTML资源文件等；

e）应对缓存在本地的程序、资源文件等进行完整性校验。

5.1.7 输入安全

5.1.7.1 客户端输入检查

客户端应对用户输入进行必要的检查，以提高用户体验，并防止意外输入被提交到服务器。

5.1.7.2 服务端参数检查

应满足以下要求：

a）恶意的用户可能会故意绕过客户端正常流程对输入参数的检查，应确保在服务器端执行所有的参数检查，不能信任客户端提交的输入参数；

b）客户端的输入的数据，包括但不限于URL参数、HTTP头、Cookie、文件等等。

5.1.7.3 防溢出攻击

服务端应验证参数的长度，防止溢出攻击。

5.1.7.4 不应信任 HTTP 头信息

HTTP头在HTTP请求和响应开始时发送。应确保服务器的任何安全决策都不是基于HTTP头中包含的信息。

5.1.7.5 防止 XSS 攻击

应满足以下要求：

a）禁止用户输入<,>等会导致XSS攻击的敏感字符；或者对敏感字符进行转义、编码后再存储；

b）源自用户输入的信息，如果需要输出到HTML页面，应先进行HTML编码；或者已经进行了上述a步骤描述的编码存储。

5.1.7.6 防止 SQL 注入

应满足以下要求：

a）禁止用户输入SQL关键词；或者对敏感字符进行转义；

b）SQL语句应以绑定变量的形式传入参数。

5.1.7.7 文件上传

服务端在接受页面上传文件时，应对文件名进行过滤，仅接受指定范围的文件（如：图片,.zip文件等），同时，应修改上传后的文件名，不应接受可能存在危险的文件（如：.jsp, .sh, .war, .jar文件等）。

如出于业务的需要（如：网盘等）必须接受任意扩展名的文件，宜避免文件可被执行，如存储时变更文件名或修改上传文件的扩展名。

应设置合理的文件上传限制策略，包括但不限于限制单个文件的合理尺寸，限制单个终端、单个IP地址、单个客户等的合理上传频率等。

5.1.7.8 安全键盘及文本输入框

用户输入C3类别的敏感信息时（如账户密码），应采用安全键盘输入，并使用特定的文本框进行字符回显，且应满足以下要求：

a）能够防范键盘窃听，能防止录屏和截屏；

b）文本框采用*字符代替原文回显；

c）逐字符加密、字符加密；

d）客户端内存中、网络传输过程，不应出现敏感信息原文；

e）密码在客户端和服务端之间传递，应采用非对称加密，服务端应能够解密并进行相关的验证，混入盐值后再采用不可逆的散列算法进行加密后存储。

5.1.7.9 避免自定义文件路径信息

服务端接收的请求中的任何内容，不应作为服务器的磁盘路径（包括相对路径）处理。

5.1.7.10 防钓鱼攻击

客户端通常会使用网页视图打开网页，应保证网址的合法性，防止被钓鱼。

应满足以下要求：

a) 宜避免使用 HTTP 协议的网址，因为 HTTP 协议的内容，容易被中间网络设备篡改内容；

b) 应设置可信域名清单，只可访问可信域名内的资源；

c) 应确保网址来源的合法性。避免打开源自用户自行输入的网址，如有，应受到可信域名清单的限制；

如网址是第三方应用通过API、或者应用拉起的方式传入（如iOS的Universal Link技术），应校验请求签名或者严格限定访问地址的域名的合法性，防止用户被钓鱼攻击。

5.1.8 密码安全

5.1.8.1 基本要求

应符合GB/T 39786—2021中的相关规定；新上线功能应使用符合国家密码主管部门要求的密码算法。

不应使用强度弱的哈希算法和加密算法，不应使用已被证明存在弱点或漏洞的加密算法。对于SSL证书，应采用强度高的加密和签名算法。

对密码采用单向哈希技术，宜避免密码泄露的风险，如高强度的哈希算法，应使用盐，避免彩虹表攻击；盐值应取自用户信息或者随机数，不应使用相同的盐值。

不应使用自定义的密码算法。

5.1.8.2 长度复杂度

应满足以下要求：

a）密码不应与手机号、证件号、生日等个人身份信息高度重合；

b）用于登录的密码，不能和用于交易验证的密码相同。应强制用户设置登录密码和交易密码。登录密码应要求一定的复杂性，最低长度限制为8位，需要包含字母、字符或者数字3种当中任意2种以上组合；

c）在身份鉴别时，应引入机密性、完整性、真实性保证的相关密码技术，包括不限于使用数字信封对敏感信息进行机密性保护、使用数字证书保护身份鉴别信息的完整性和真实性；

d）若采用手势密码作为验证要素，手势密码应至少设置连续不间断的4个点。

5.1.8.3 密钥管理

应满足以下要求：

a）密钥(对)在传输过程中应使用密码算法对密钥(对)进行保护；

b）随机生成的密钥(对)应具有一定的随机性与不可预测性；

c）密钥(对)应加密存储，并确保密钥(对)存储位置和形式的安全；

d）在客户端使用数字证书或者应用加固技术防止非对称密码算法公钥被篡改。

5.1.8.4 密钥专用

应满足以下要求：

a）不同移动互联网应用程序中，应使用不相关的密钥(对)；

b）不同安全用途的业务场景中，应使用不相关的密钥(对)；

c）对接不同的合作渠道时，应使用不相关的密钥(对)；

d）不同的应用环境(开发、测试、生产)，应使用不相关的密钥(对)。

5.1.8.5 密钥更换

不宜长期使用同一密钥(对)，应为密钥(对)设定有效期，并及时更换。

5.1.9 组件安全

应满足以下要求：

a）宜避免使用存在已知漏洞的系统组件与第三方组件；

b）宜避免第三方组件未经授权收集移动互联网应用程序信息和个人信息。如确需收集，应在隐私政策中逐一明示各组件收集与使用个人信息的目的、方式、范围，并征得用户同意；

c）应确保第三方组件有合法来源和持续使用的授权；

d）应持续对第三方组件进行安全扫描；

e）应定期升级更新第三方组件版本确保其可用性；

f）应开展安全评估等方式，防止第三方代码(组件)收集与用户使用的产品或服务无关的个人信息。

5.1.10 日志安全

5.1.10.1 客户端日志

应满足以下要求：

a）生产环境正式发布的客户端，应默认关闭日志输出功能；

b）如因诊断问题需要，可在用户的授权下将日志输出到文件，并加密上传到服务器进行分析。且日志中不应包含敏感信息；
c）采用密码技术，对日志进行完整性保护，如可信时间戳服务等；
d）应确保相关日志中没有记录密码或其他敏感数据。

5.1.10.2 服务端日志

服务异常时，不应暴露错误堆栈信息、中间件信息、函数名等可能会被用于攻击的关键信息，应向用户展示自定义的友好信息。

5.2 用户个人信息安全

5.2.1 个人信息收集的总体原则

个人信息的收集，应符合GB/T 35273—2020、JR/T 0171—2020中的规定。

5.2.2 收集个人信息的合法性要求

应满足以下要求：
a）不应误导、欺诈、诱骗、强迫个人信息主体提供其个人信息；
b）不应隐瞒产品或服务所具有的收集个人信息的功能；
c）不应从非法渠道获取个人信息；
d）不应收集法律法规明令禁止收集的个人信息。

5.2.3 收集个人信息的最小化要求

应满足以下要求：
a）收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现；
b）自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；
c）间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

5.2.4 收集个人信息的授权同意

应满足以下要求：
a）收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则（如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等），并获得个人信息主体的授权同意；
b）间接获取个人信息时：
1)应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；
2)应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等。如本组织开展业务需进行的个人信息处理活动超出该授权同意范围，应在处理个人信息前，征得个人信息主体的明示同意。

5.2.5 收集个人敏感信息的明示同意

应满足以下要求：

a）收集个人敏感信息时，应取得个人信息主体的单独明示同意。应确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的意思表示；

b）通过主动提供或自动采集方式收集个人敏感信息前，应向个人信息主体告知所提供产品或服务的核心业务功能及所必需收集的个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响；应允许个人信息主体选择是否提供或同意自动采集；

c）产品或服务如提供其他附加功能，需要收集个人敏感信息时，收集前应向个人信息主体逐一说明个人敏感信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时，可不提供相应的附加功能，但不应以此为理由停止提供核心业务功能，并应保障相应的服务质量；

d）收集年满 14 周岁的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意。

5.2.6 隐私政策的内容和发布

应满足以下要求：

a）隐私政策应包含个人信息处理者的基本情况，包括公司名称、联系地址、联系方式等；

b）隐私政策应包含收集、使用个人信息的目的，以及目的所涵盖的各个业务功能，如将个人信息用于推送商业广告、将个人信息用于形成直接用户画像及其用途等；

c）隐私政策应包含各业务功能分别收集的个人信息范围，以及收集方式和频率、存放地域、存储期限等个人信息处理规则；

d）隐私政策应包含对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及所承担的相应法律责任；

e）隐私政策应包含遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施；

f）隐私政策应包含个人信息主体的权利和实现机制，如访问方法、更正方法、删除方法、注销账户的方法、撤回同意的方法、获取个人信息副本的方法、约束信息系统自动决策的方法等；

g）隐私政策应包含提供个人信息后可能存在的安全风险，以及不提供个人信息可能产生的影响；

h）隐私政策应包含处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式；

i）隐私政策所告知的信息应真实、准确、完整；

j）隐私政策的内容应清晰易懂、符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言，并在起始部分提供摘要，简述告知内容的重点；

k）隐私政策应公开发布且易于访问，如在移动应用程序安装页等显著位置设置访问链接；

l）隐私政策应逐一送达个人信息主体。当成本过高或有显著困难时，可以公告的形式发布；

m）在本条 a)所载事项发生变化时，应及时更新隐私政策并重新告知个人信息主体。

n）在移动互联网应用程序首次运行时应通过弹窗等明显方式提示用户阅读隐私政策；

o）宜避免出现隐私政策难以访问的情况，如进入移动互联网应用程序主界面后，访问隐私政策的操作步骤大于4步；

p）宜避免出现隐私政策难以阅读的情况，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

6 移动互联网应用程序兼容性、性能和交互要求

6.1 兼容性要求

6.1.1 操作系统版本

宜适当考虑使用低版本系统的用户能正常使用移动互联网应用程序的主要功能，基本要求如下：

a）针对Android和iOS操作系统版本的兼容,应分别覆盖Android和iOS发布的按版本时序排列的累计市场占有率超过95%的操作系统版本；

b）支持鸿蒙操作系统；

c）如条件许可，可支持其他有需求的操作系统；

d）最低操作系统版本支持，应根据市场设备、系统占有率、客户实际情况等最新信息，每年进行调整。

6.1.2 硬件兼容性要求

移动互联网应用程序应适配主流的手机设备品牌和型号,应在不同屏幕尺寸的手机上正确显示和运行。

6.1.3 网络环境

移动互联网应用程序应支持主流运营商网络访问，同时支持IPv4和IPv6，优先使用IPv6与服务器建立连接，当IPv6网络环境异常时，切换至IPv4。

6.1.4 软件共存

移动互联网应用程序应能独立完成安装使用，不应依赖任何第三方完成安装，且支持与其他移动互联网应用程序共存。

6.2 性能要求

6.2.1 安装包文件大小

应控制安装包的大小，方便用户能轻易下载使用。可根据业务发展情况慎重调整安装包大小。

6.2.2 安装包文件优化

安装包内的文件应从多方面进行优化，降低包文件的大小，优化方法不限于如下内容：

a）宜对应用程序资源文件进行优化，方法不限于删除冗余资源、压缩图片资源等；

b）宜对可执行文件进行优化，方法不限于排除第三方SDK无用依赖库、重构封装以精简代码、开启代码混淆压缩代码、清除数据结构中的取值赋值方法等；

c）宜对资源库进行优化，方法不限于只提供对主流架构的支持。

6.2.3 冷启动时间

应控制移动互联网应用程序在主流移动设备上的冷启动时间，充分保障用户良好体验。

6.2.4 服务器响应时间

后台服务器应对移动互联网应用程序的请求进行快速响应，尤其在系统访问高峰时间段，接口的平均响应速度应结合实际并发情况合理优化，充分保障用户的良好体验。

6.2.5 服务器并发量

后台服务器在架构设计上应遵循高并发、高可用原则，应结合历史访问量及系统压测情况，保证合理的系统并发处理能力；结合企业自身峰值时间，计算峰值时间每秒请求数(QPS)，系统压测QPS宜不低于历史峰值QPS的3倍，最大承受在线用户数、每分钟最大交易笔数等核心指标宜不低于历史峰值3倍；应定期对系统进行重新压测和容量评估，按标准及时进行系统调整。

6.2.6 CPU 占用率

应合理使用终端设备的CPU，在主流设备上使用一般功能时的CPU占有率不宜持续过高，确保与其他移动互联网应用程序间稳定切换使用，防止系统卡顿、死机等现象。

6.2.7 内存占用率

应合理使用终端设备的内存，具体来说，在主流设备上使用一般功能时的内存占有率应维持平稳，不宜持续升高，采取措施包括但不限于：

a) 及时回收无用资源；

b) 使用第三方检测工具检测内存使用情况、确保应用无内存泄露。

6.2.8 耗电量

移动互联网应用程序应采取措施控制运行时耗电量，包括但不限于：

a) 平衡客户端和服务端的复杂业务处理，合理减少客户端压力；

b) 避免前后端频繁交互，减少耗时网络请求。

6.2.9 流量控制

移动互联网应用程序宜避免消耗较多的数据流量，在业务场景允许的情况下，宜尽量压缩报文的大小。对于大文件下载且网络环境非无线网络的场景下，需要额外获取到用户的授权。

6.2.10 服务降级和熔断

移动互联网应用程序应结合具体的业务场景，采用适当的服务降级方案，如页面降级、服务降级、限流降级等，保障核心服务可用，提升用户体验。

移动互联网应用程序应结合具体服务重要程度，采用适当的服务熔断机制，健全链路保护，防止系统崩溃。

6.3 交互要求

6.3.1 交互总体要求

移动互联网应用程序交互设计应符合用户交互习惯，交互层级清晰且控制在适当范围内，界面简洁易于理解，遵循公司设计规范。

移动互联网应用程序交互设计应关注适老化改造，符合JR/T 0246—2022相关要求，如为老年用户适当增大字体大小、提供语音输入功能等。

6.3.2 消息推送要求

移动互联网应用程序消息推送应支持用户对推送功能进行自定义管理：

a) 应对推送消息进行合理分类；

b) 应允许用户针对不同分类消息进行开关设置；

c) 宜对消息推送方式进行自定义设置，如声音开关、震动开关、免打扰模式等。

6.3.3 交互安全

6.3.3.1 客户端进入后台提示

客户端进入后台运行时，应提醒用户应用已进入到后台，防止用户界面劫持攻击。在后台运行的客户端应用程序，应对应用预览画面进行模糊化处理。

6.3.3.2 截屏录屏提醒

在输入密码时，如有截屏录屏动作，应提醒用户。在录屏过程中，在涉及密码等敏感信息输入界面时，宜根据手机系统专有能力分别进行录制黑屏、拦截等处理。

6.3.3.3 客户端敏感信息展示

客户敏感身份信息与交易敏感数据信息等作为一般性浏览用途时，应进行掩码脱敏处理，且掩码脱敏处理应在服务端实现；应提供针对脱敏信息进一步查询原始信息的功能，用户需要查询原始信息时，需要完成增强的身份认证流程。

7 移动互联网应用程序管理要求

7.1 研发管理

7.1.1 研发管理的基本要求

移动互联网应用程序的研发管理，应符合JR/T 0092—2019中6.2、6.3的规定及相关监管要求。

7.1.2 项目管理要求

移动互联网应用程序应执行严格的项目管理流程，且项目管理流程应覆盖客户端的需求、开发、测试、发布上线等全项目周期环节，各个环节均应交付相关文档，如：软件需求说明书、系统设计说明书、测试用例设计书、测试验收报告、系统发布上线操作手册和用户使用手册等。

如条件许可，宜尽量保证项目组各环节参与人均能在项目初期即参与到项目中，以保证项目组成员对项目目标的对齐统一，提高项目交付质量。

7.1.3 软件开发要求

7.1.3.1 软件开发基本要求

移动互联网应用程序的开发，应遵循统一严格的编码规范；应建立静态代码扫描机制，对于代码扫描排查出的问题，应及时安排处理；应建立人工评审机制，定期组织代码评审，持续关注并提升软件代码质量。

7.1.4 软件测试要求

7.1.4.1 软件测试基本要求

应满足以下要求：

a）针对软件需求，应设计充分的测试用例，并与需求、开发人员进行确认；
b）测试执行阶段应覆盖全部测试用例，测试缺陷应关联具体的测试用例；
c）应建立可行有效的缺陷管理机制，对不同程度的缺陷设计合理的缺陷应对策略。

7.1.4.2 缺陷应对策略

缺陷应对策略应匹配缺陷影响程度和缺陷影响范围：
a）对于导致系统崩溃、应用无法启动、核心数据破坏或丢失等全局问题的缺陷，应分配最高的解决时效要求，并充分分析问题产生原因与未来规避方案；
b）对于导致功能实现缺失、核心业务逻辑错误、数据无法保存等局部严重问题的缺陷，应分配较高的解决时效要求，并在当期版本进行解决；
c）对于导致功能实现与需求存在差异、程序健壮性不足、边界和异常数据处理不正确、页面展示内容错误等局部一般问题的缺陷，如当期修复难度或成本较高，应在项目组范围内进行审慎评估后遗留至后续版本解决，并应针对缺陷设计弥补方案；
d）对于导致功能实现与需求存在微小而不影响实质的差异、影响操作易用性，以及一些建议优化的问题的缺陷，如当期修复难度或成本较高，可遗留至后续版本解决。

7.1.5 软件发布要求

应制定详细的发布流程规范。

7.1.5.1 软件发布前准备

应满足以下要求：
a）发布前应移除测试或调试目的的代码逻辑、数据和配置项；
b）应进行必要的代码混淆和应用加固，以防范攻击者对客户端程序的逆向、分析和篡改；
c）应检查客户端的名称、版本、图标等信息是否正确；
d）应提供必要的版本更新内容说明；
e）应使用企业证书对客户端进行签名；
f）如条件许可，在客户端软件正式发布之前，应进行生产环境的灰度发布和验证。

7.1.5.2 软件发布

应满足以下要求：
a）客户端软件应在主流应用商店上架发布，并提供独立的自有发布和升级方式；
b）应对不同客户端版本的客户覆盖率进行有效统计，客户端软件宜尽量对过往主要版本进行兼容，如在具体功能层面无法兼容，则应在客户需要使用具体功能时才要求客户升级，应谨慎实施整个客户端软件层面的强制升级；
c）客户端软件对操作系统的权限申请应遵循最小必要原则，并提供申请权限的必要性说明，基础权限在软件安装时进行授权，非基础权限应该在使用到相应功能时再进行授权。

7.2 运维管理

7.2.1 运维管理的基本要求

移动互联网应用程序的运维管理，应符合JR/T 0092—2019中6.4的规定及相关监管要求。

7.2.2 基础设施和网络运维管理要求

应满足以下要求：

a）应为服务端提供高可用高可靠的基础设施环境，不应存在单点故障问题风险，集群服务宜尽量跨机器、跨机架部署；
b）应使用安全可靠的通讯协议进行网络通讯，宜使用基于公认安全加密算法的HTTPS协议进行通讯；
c）安全证书应按时更新，避免因为证书过期导致的服务不可用问题；
d）应支持主流运营商网络进行访问，且同时支持IPv4协议和IPv6协议；
e）应对服务端环境的重要技术指标（包括但不限于CPU使用率、内存磁盘空间使用率、吞吐量、输入输出指标等）和网络联通情况进行持续有效的监控。

7.2.3 应用运维管理要求

应满足以下要求：
a）系统升级、数据变更等重大应用运维操作，应当记录详细的运维操作记录；
b）应定期以及在重大版本变更上线后，组织针对应用系统的安全扫描和渗透测试；
c）应持续关注主流漏洞平台发布的重大漏洞情况，并及时组织针对应用系统的自查和修复；
d）应对服务端应用运行情况（包括但不限于服务可用性、性能指标、请求数、会话数、异常日志等）进行持续有效的监控；
e）在客户授权的前提下，客户端应能上报异常日志，应定期分析客户端上报的异常日志，针对客户端异常、闪退、性能下降等问题进行跟踪处理。

8 移动互联网应用程序创新应用

8.1 总体原则

依托大数据、云计算、区块链、人工智能等技术，在满足监管合规的前提下，结合客户多元化需求，移动互联网应用程序可在业务流程、用户体验、安全风控、适老化改造等方面进行创新。

8.2 生物特征识别

可将生物特征识别技术应用在移动互联网应用程序的安全验证业务流程中，通过加密等技术手段充分保障用户生物特征的隐私安全。

8.3 人脸活体检测

在某些对安全性要求较高的业务场景（如找回密码、在线换卡）中，移动互联网应用程序可采取活体检测技术，与公安部等权威渠道进行人脸、证件合一的比对验证。

8.4 OCR 识别

移动互联网应用程序可将OCR文字识别技术恰当地运用在银行卡、身份证等信息的采集过程中，同时，OCR识别应具备一定的防伪性和易用性。

8.5 语音识别

移动互联网应用程序可将语音识别技术恰当地运用在信息输入、信息搜索、客服问答等场景中，赋能适老化及无障碍服务领域，包括但不限于：

a）支持通过智能语音助手交互及反馈，完成业务办理；

b）支持语音搜索服务，客户输入语音方式进行搜索；

c）语音搜索应支持搜索结果通过图文形式对用户展现。

8.6 智能问答

可通过深度学习、自然语言处理等人工智能技术，对接智能问答系统，实现自动化、智能化运营，为客户提供全天候、快速高效的服务。

参 考 文 献

[1] 《中华人民共和国个人信息保护法》 2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过

[2] 国家互联网信息办公室秘书局.APP违法违规收集使用个人信息行为认定方法. 2019-12-30

[3] 国家互联网信息办公室.移动互联网应用程序信息服务管理规定.2022-06-14

[4] 国家互联网信息办公室，工业和信息化部，国家市场监督管理总局.互联网弹窗信息推送服务管理规定.2022-09-09

[5] 《证券期货业网络和信息安全管理办法》 2023年1月17日中国证券监督管理委员会第1次委务会议审议通过