ICS 03.060
CCS A 11

Q/HRCB

江苏海安农村商业银行股份有限公司企业标准

Q/HRCB 002—2023
代替 Q/HRCB 002—2022

移动金融客户端应用软件安全管理规范

Safety management standards For Financial Mobile Application Software

2023－04－04 发布　　2023－04-04 实施

江苏海安农村商业银行股份有限公司
发 布

目　　次

前　言

互联网金融平台业务发展迅速，为了保证业务安全可靠，规避风险，就产品的业务安全稳定性方面制定本文件。

本文件根据GB/T 1.1-2009给出的规则起草。

本文件由江苏海安农村商业银行股份有限公司提出并归口。

本文件起草单位： 江苏海安农村商业银行股份有限公司。

本文件主要起草人：吴智星、朱骞、刘飞。

本文件的历次发布情况为：

——2019年首次发布。

——2020年第一次修订。

——2021年第二次修订。

——2022年第三次修订。

——本次为第四次修订。

移动金融客户端应用软件安全管理规范

1 范围

本文件规定了移动金融客户端应用软件的安全要求，以及客户端应用软件设计、开发、维护和发布的管理要求。

本文件适用于本行所有的移动金融客户端应用软件的设计、开发、维护及发布过程。

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。

JR/T 0092—2019 《移动金融客户端应用软件安全管理规范》

JR/T 0171—2020 《个人金融信息保护技术规范》

3 术语与定义

3.1

移动金融客户端应用软件

移动金融客户端应用软件(financial mobile application software)，指在移动终端上为用户提供金融交易服务的应用软件,包括但不限于可执行文件、组件等。

3.2

资金交易类客户端应用软件

资金交易类客户端应用软件(capital transaction client application software)，指直接面向用户提供资金交易服务的移动金融客户端应用软件,包括但不限于手机银行、支付APP等。

3.3

信息采集类客户端应用软件

信息采集类客户端应用软件(information collection client application software)，指不直接向用户提供资金交易服务，但需采集个人敏感信息的移动金融客户端应用软件。

3.4

资讯查询类客户端应用软件

资讯查询类客户端应用软件(information query client application software)，指仅提供金融产品推介、信息查询、资讯推送等服务的移动金融客户端应用软件。

3.5

个人金融信息

个人金融信息(personal financial information)，是指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，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。

3.6

支付敏感信息

支付敏感信息(payment sensitive information)，指支付信息中涉及支付主体隐私和身份识别的重要信息， 包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

4 总体要求

移动金融客户端应用软件分为三类，分别是资金交易类、信息采集类和资讯查询类：

a) 资金交易类客户端应用软件原则上应符合客户端应用软件所有安全及管理要求；

b) 信息采集类客户端应用软件原则上应重点符合客户端应用软件与信息保护相关安全及管理要求；

c) 资讯查询类客户端应用软件参照执行相关客户端应用软件安全及管理要求。

5 客户端应用软件安全要求

5.1 身份认证安全

5.1.1 认证方式

a) 电子认证应组合选用下列三类要素中的两类或者三类：

1) 仅客户本人知悉的要素，如静态密码等；

2) 仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；

3) 客户本人生物特性要素，如指纹等。

b) 对于手势密码、短信验证码、生物特征信息作为验证要素或验证要素组合中的一种时，应满足如下要求：

1) 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；

2) 采用短信验证码作为验证要素，短信验证码应仅使用一次，仅限于在规定时间内使用，短信验证码应具备长度和随机性的要求,短信验证码所在的短信内容中,告知用户短信验证码的用途；

3) 采用生物特征识别作为验证要素,应当符合国家、金融行业标准和相关信息安全管理要求，防止非法存储、复制和重放。

c) 必须确保采用的身份验证要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露；

5.1.2 认证信息安全

5.1.2.1 安全输入

客户端应用软件应提供客户输入银行卡支付密码和网络支付交易密码的即时防护功能，客户端应提供以下安全控制措施，或其他经攻击测试无法获取明文的安全防护措施。

a) 采取替换输入框原文；
b) 逐字符加密、字符加密；
c) 防范键盘窃听；
d) 采用自定义软键盘；
e) 客户端应用软件应实现防截屏、录屏的功能。

5.1.2.2 个人金融信息展示

a) 客户端应用软件的口令框应默认屏蔽显示，屏蔽显示时应使用同一特殊字符（例如*或•） 代替；
b) 客户端应用软件不应明文显示银行卡密码和网络支付交易密码；
c) 客户端应用软件展示个人金融信息时， 应符合以下要求：

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，并做好此类信息管理，防范此类信息泄露风险。用户处于未登录状态时，不应展示与个人信息主体相关的用户鉴别信息（如：银行卡账号、卡片有效期、登录密码、支付密码等）。

5.1.3 认证失败处理

a) 客户端应用软件应提供认证失败处理功能，可采取结束会话、限制失败登录次数和自动退出等措施；
b) 在提示客户认证失败时，应模糊错误提示信息，防止错误提示信息中泄露用户全部账号、交易金额等敏感数据。

5.1.4 密码的设定与重置

a) 客户端应用软件应配合服务端提供密码复杂度校验功能，保证用户设置的密码达到一定的强度，避免采用简单交易密码或与客户个人信息相似度过高的交易密码；
b) 应严格限制使用初始登录密码与初始交易密码，若设置初始密码，应强制用户在首次登录后修改初始密码；
c) 在修改密码前，应对用户身份进行重新验证；
d) 修改密码时，应对原密码输入错误次数进行限制；
e) 修改密码时，新密码不应与原密码相同；
f) 在密码重置时，必须使用短信验证码、用户注册信息校核等方式，对用户身份进行校验。

5.2 逻辑安全

5.2.1 逻辑安全设计

a) 对于认证、校验等安全保证功能的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绕过；
b) 对于交易处理功能逻辑设计应充分考虑其合理性，避免逻辑漏洞的出现，保证资金交易安全；
c) 客户端代码实现应尽量避免调用存在安全漏洞的函数，避免敏感数据硬编码。

5.2.2 软件权限控制

客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。

5.2.3 风险控制

a) 应设计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；

2）针对不同的资金交易业务场景，应设计合理的策略，如：限额控制策略、不同认证方式策略等。

b) 客户端应用软件应配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统。

5.2.4 回退处理

交易过程中如遇交易失败或在交易完成前用户进行撤销操作，应返回到交易前的有效状态。

5.2.5 异常处理

a) 客户端应用软件发生故障产生的异常信息，不应泄露用户的敏感数据；

b) 当交易出现异常时，客户端应用软件应向客户提示出错等信息，但不应泄露用户的敏感数据。

5.3 安全功能设计

5.3.1 组件安全

a) 客户端应用软件应避免使用存在已知漏洞的系统组件与第三方组件；

b) 客户端应用软件在使用第三方组件时，应避免第三方组件未经授权收集客户端应用软件信息和个人信息。

5.3.2 接口安全

客户端应用软件应对软件接口进行保护，防止其他应用对客户端应用软件接口进行非授权调用。

5.3.3 抗攻击能力

a) 客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作；

b) 客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护；

c) 客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力；

d) 客户端应用软件如使用安全输入控件，该控件应具备抵御一定程度攻击的能力。

5.4 密码算法及密钥管理

5.4.1 密码算法

a) 客户端应用软件应使用密码算法对资金有关交易或重要业务操作进行保护；

b) 密码算法、密钥长度及密钥管理方式应符合国家密码主管部门的要求。

5.4.2 密钥管理

a) 密钥在传输过程中应使用密码算法对密钥进行保护；

b) 随机生成的密钥应具有一定的随机性与不可预测性；

c) 密钥应加密存储，并确保密钥储存位置和形式的安全。

5.5 数据安全

5.5.1 数据获取

5.5.1.1 数据防窃取

a) 客户端应用软件应保证内存中不应存在完整的银行卡密码和网络支付交易密码明文；

b) 客户端应用软件的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) 客户端应用软件程序应禁止在身份认证结束后存储支付敏感信息， 防止支付敏感信息泄露；

d) 客户端应用软件运行日志中不应打印支付敏感信息、不应打印完整的敏感数据原文；

e) 应采取技术手段防止内存中加密的敏感数据被还原为明文。

5.5.1.2 数据防篡改

用户输入关键交易数据时，如：收款人信息、交易金额、订单号等，应采取防篡改机制保证数据不被移动终端的其他程序篡改。

5.5.1.3 数据有效性

客户端应用软件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。

5.5.2 数据访问控制

a) 应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问；

b) 客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。

5.5.3 数据传输

5.5.3.1 通讯安全

a) 应在客户端应用软件与服务器之间建立安全的信息传输通道，协议版本应及时更新至安全稳定版本；

b) 应确保采用的安全协议不包含已知的公开漏洞；

c) 客户端应用软件与服务器应采用 SSL 协议认证，可通过密钥、证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。

5.5.3.2 数据保密性

a) 敏感数据（如：登录口令、支付敏感信息等）在客户端应用软件与本地其他应用软件间传输时，应采取加密等措施确保其保密性，若本地其他应用软件不能提供与金融客户端软件相应等级的加密接口，则应评估敏感数据调用的风险，并设计补救措施；

b) 敏感数据（如：登录口令、支付敏感信息等）在通过公共网络传输时，应采取加密等措施确保其保密性。

5.5.3.3 数据完整性

a) 关键的交易数据，如：收款人信息、交易金额、订单号等，在客户端应用软件与本地其他应用软件间传输时，应采取措施（如：数字签名、MAC 等）确保其完整性，若本地其他应用软件不能提供与金融客户端软件相应等级的数据完整性保护措施，则应评估关键数据传输的风险，并设计补救措施；

b) 关键的交易数据、个人身份信息，如：收款人信息、交易金额、订单号、身份证号码等，在通

过公共网络传输时，应采取措施（如：数字签名、MAC 等）确保其完整性。

5.5.3.4 数据抗抵赖

通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术。

5.5.3.5 数据防重放

通过客户端应用软件发起的身份认证或资金类交易报文，应能够防止重放攻击。

5.5.4 数据存储

5.5.4.1 个人金融信息存储

a) 客户端应用软件不应以任何形式存储用户的支付敏感信息与金融业务查询口令；

b) 客户端应用软件应向个人金融信息主体告知共享、转让个人金融信息的目的、个人金融信息接收方的类型，并事先征得个人金融信息主体明示同意；

c) 在满足法律、管理规定的前提下，客户端应用软件应仅保存业务必需的个人金融信息，并限制数据存储量；

d) 在个人金融信息加工处理的过程中，应建立个人金融信息防泄露控制规范和机制，防止个人金融信息处理过程中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息。

5.5.4.2 加密密钥存储

客户端应用软件应确保无法通过逆向工程等手段直接从本地文件系统中恢复完整的密钥明文。

5.5.5 数据展示

除交易对账、转账收款方确认等必须由用户确认的情况外， 客户端应用软件在显示个人信息，如：银行账号时应屏蔽关键字段。

5.5.6 数据销毁

5.5.6.1 残余信息保护

a) 客户端应用软件应在敏感数据使用完毕后，对其立即进行清除；

b) 客户端应用软件进程被结束时，应清除非业务功能运行所必需留存的业务数据，保证客户信息的安全性；

c) 客户端应用软件卸载完成后，文件系统中不应残留任何个人金融信息。

5.5.6.2 会话失效

客户端应用软件在安全退出登录时，应向服务器发送会话结束请求，使当前会话状态失效。

5.6 身份认证的口令必须动态更换

所有需要登录才能操作的接口，必须要有身份认证。身份认证采用动态口令，有效期不能超过20分钟。

6 客户端应用软件管理要求

6.1 设计要求

a) 客户端应用软件设计应遵循安全、可靠、易用、可维护和可扩展等原则，制定用于指导客户端应用软件设计与开发的总体方案。客户端应用软件应提供易用、风格统一、体验良好的用户界面；

b) 客户端应设计适合老年人使用，坚持传统服务方式与智能化服务创新并行，切实解决老年人在运用智能技术方面遇到的困难。

c) 客户端应采取技术措施（如弹窗、明显位置 URL 链接等），引导个人金融信息主体查阅隐私政策，并获得其明示同意后，开展有关个人金融信息的收集活动；

d) 客户端应遵循合法、正当、必要的原则，向个人金融信息主体明示收集与使用个人金融信息的目的、方式、范围和规则等，不得收集与所提供服务无关的个人金融信息；

e) 客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除；

f) 客户端应用软件应提供访问、更正个人金融信息，以及授权撤销、账户注销等功能；

g) 面向客户使用的移动客户端时，应充分考虑移动端系统兼容性，安卓系统须最低支持安卓 6.0 版本（含 6.0），IOS 系统最低须支持 IOS 9（含 IOS 9）版本；

h) 客户端应用必须能够在仅支持 IPv6 的网络上完全正常地运作；

i) 面向客户使用的移动应用，应用程序内应公布联系信息，以便用户与客服联系；

j) 在移动客户端中不应包含未记录的功能或隐藏功能；

k) 客户端应用软件安装包文件大小不应超过 120MB；

l) 客户端应用软件冷启动时间<=2 秒；客户端应用软件的后台服务器相应时间<=1 秒, 客户端应用软件的后台服务器支持并发>=1000；

m) 客户端应用软件 CPU 占有率<=0.1%, 客户端应用软件内存占有率<=5%；

n) 移动金融客户端软件在安装时与其它正在运行的移动金融客户端软件之间允许共存。 支持与其它独立移动客户端软件（移动客户端杀毒软件等）共存；

o) 若移动金融客户端采用指纹识别技术作为登录或支付的验证方式， 则在指纹特征识别系统错误拒绝率<=3%的情况下，错误接受率应<=0.001%；

p) 若移动金融客户端采用人脸识别技术作为登录或支付的验证方式， 则在人脸特征识别系统错误拒绝率<=5%的情况下，错误接受率应<=0.1%；

q) 若移动金融客户端采用声纹识别技术作为登录或支付的验证方式， 则在声纹特征识别系统错误拒绝率<=3%的情况下，错误接受率应<=0.5%。

6.2 开发要求

a) 客户端应用软件开发过程中应遵守严格的开发流程、项目管理流程和编码安全规范，进行完整的测试，避免在请求、响应、存储、配置等功能中存在漏洞；

b) 客户端应用软件开发过程中应建立并维护开发文档，应同步完成产品手册、用户手册或提供在线帮助说明功能；

c) 客户端应用软件的每次重大版本更新、升级，都必须经过严格归档、源代码扫描、发布审核等步骤。

6.3 测试要求

a) 在系统开发测试过程中，应对开发测试环境与生产环境进行有效隔离；

b）开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化（不应仅使用加密技术）脱敏处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需个人金融信息除外。

6.4 发布要求

a) 客户端应用软件应有规范的上线发布流程，由应用软件的所有方对应用软件进行签名和保护，标识应用软件的来源和发布者，提供安全可靠的应用软件下载、发布、升级渠道；

b) 客户端应用软件应当删除调试或测试中存留的敏感数据；

c) 客户端应用软件有新版本时，不能未经用户允许自动安装新版本；

d) 客户端有新版本升级，应提前请符合要求的测试机构进行兼容性测试和渗透测试并出具相应报告。

6.5 维护要求

a) 应制定科学、合理的管理策略和执行制度，指导各类角色的工作协同、实施步骤、质量管控、安全检测等，规范日常运维流程；

b) 客户端应用软件应具有明确的应用标识符和版本序号，设计合理的更新接口，当某一版本被证明存在安全隐患时，应及时进行修复更新；

c) 后台服务端需要升级前，须走审批流程，流程结束后方可升级。

6.6 上线授权和审批

应针对移动金融客户端应用业务及技术规划、架构及策略、移动金融客户端应用新产品推出、移动金融客户端应用重要技术路线选择、移动金融客户端应用系统重要变更操作、物理访问和移动金融客户端应用系统接入等事项建立审批程序，应提交高级管理层审批，并按照审批程序执行审批过程，对重要活动建立逐级审批制度。