Q/zxjtqhapp

中 信 建 投 期 货 企 业 标 准

Q/zxjtqhapp 001—2021

移动金融客户端技术要求

Financial mobile application technical requiremen

2021 - 07 - 30 发布　　2021 - 07 - 30 实施

信息技术部 发布

目　　次

前　言

本标准按照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》、JR/T 0092-2019《移动金融客户端应用软件应用软件安全管理规范》、JR/T 0192-2020《证券期货业移动互联网应用程序安全规范》等相关规定起草。

本标准根据期货移动金融客户端应用软件的实际情况，参考有关行业标准而制定。

本标准由中信建投期货有限公司归口。

本标准起草单位：中信建投期货有限公司信息技术部。

本标准主要起草人：谢乔如、张恒、颜韵。

引　　言

移动金融是新时期移动互联网时代金融信息化发展的必然趋势，移动金融客户端应用软件的建设是金融信息化建设的重中之重，在移动互联网时代，移动金融客户端应用软件安全运行的压力越来越大，所面临的信息安全形势日趋复杂。移动金融客户端应用软件安全、管理和运营方面的问题尤其严峻。

移动金融客户端应用软件技术要求对规范中信建投期货有限公司客户端的开发、发布、管理具有指导作用，保护金融客户隐私信息，减少设计缺陷和安全漏洞，强化个人金融信息风险识别和监控，提升安全运营水平。

中信建投期货移动金融客户端应用软件技术要求

1 范围

本标准规定了移动金融客户端应用软件的安全及管理要求，同时确立了客户端应用软件的设计开发、测试、发布更新、维护及创新的总体原则。

本标准适用于中信建投期货有限公司发布的移动金融客户端应用软件。

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，仅所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。

JR/T 0092-2019《移动金融客户端应用软件安全管理规范》

JR/T 0192-2020《证券期货业移动互联网应用程序安全规范》

JR/T 0171-2020《个人金融信息保护技术规范》

JR/T 0191-2020《证券期货业软件测试指南软件安全测试》

3 定义和术语

GB/T 25069—2010、GB/T 22239—2008和JR/T 0060—2010界定的以及下列术语和定义适用于本文件。

3.1

移动金融客户端软件 financial mobile application software

在移动终端上为用户提供金融交易服务的应用软件。

注：移动金融客户端应用软件通常由可执行文件、组件组成。

3.2

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：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

4 移动金融客户端应用软件安全要求

4.1 身份认证安全

4.1.1 认证方式

应符合JR/T 019-2020《证券期货业移动互联网应用程序安全规范》，移动金融客户端应用软件满足以下鉴别认证方式，安全技术要求：

a).对于资金类交易、客户信息修改等关键业务，增设二次认证的环节，且不应仅使用存放在移动客户端的本地信息进行认证。认证方式包括密码、生物特征、短信、令牌、图形手势等中的至少一种；

b).若采用第三方移动互联网应用程序的认证方式，移动金融客户端应用软件应再次进行用户名密码登记并核验；

c).应采取限定连续登录失败次数的措施，如设置登录失败次数上限、多次登录失败后的账户锁定策略等；

d).应具备登录超时锁定或注销功能，在设定的时间段内没有任何操作的情况下，终止登录会话，需要再次进行身份鉴别才能够重新操作。

4.1.2 认证数据保护

应符合JR/T 019-2020《证券期货业移动互联网应用程序安全规范》，认证数据保护应提供以下功能：

a).未授权不允许查阅或修改关键业务数据；

b).对于资金类交易、客户信息修改等关键业务应通过短信等多媒体方式对用户进行提醒；

c).身份认证绑定对象为用户身份信息，不局限移动终端的设备单一信息。

4.1.3 认证失败处理

应符合JR/T 0092-2019《移动金融客户端应用软件应用软件安全管理规范》，认证失败处理满足以下要求：

a).客户端应提供认证失败处理功能，采取限制失败登录次数措施；

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。

4.1.4 密码安全

保障密码的安全性，满足以下安全性要求：

a).密码不应以任何形式明文保存在APP客户端的本地存储上；

b).密码在传输过程不应以明文的形式传输，宜采用国密算法或国际数据加密算法；

c).密码输入框默认禁止明文显示密码；

d).输入静态密码时不应长时间回显，需要使用特定符号（如：“*”或“·”）替代；

e).登录密码的限制：需要有长度和复杂度控制；

- 基本概念：四类字符（大写字母，小写字母，数字，特殊符号）。
- 口令要求：长度8以上，包含两类字符。

f).密码禁止在缓存和日志中输出；

g).对密码修改前验证用户身份；

h).提供客户输入信息时的即时防护功能，防止重要信息被盗取。

4.2 个人金融信息保护

应符合JR/T 0092-2019《移动金融客户端应用软件应用软件安全管理规范》，移动金融客户端应用软件满足以下要求：

a) 客户端的口令框默认屏蔽展示，屏蔽显示时应使用同一特殊字符（“*”或“·”）代替；

b) 客户端不应明文显示期货、基金、银行等交易密码；

c) 客户端展示个人金融信息时，应符合以下要求：

- 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：卡片验证码、卡片有效期、登录密码、银期转账密码、支付密码等）；
- 处于已登录状态时，个人金融信息展示的技术要求如下：
  - ◆ 除银行卡有效期外，用户鉴别信息（如：卡片验证码、登录密码、银期转账密码、支付密码等）不应明文展示；
  - ◆ 对于客户法定名称、资金账号、银行卡号、手机号码、证件类或其他识别标识信息等可以直接或组合后确定信息主体的信息应及进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应履行客户端身份验证，并做好此类信息管理，防范此类信息泄露风险；
  - ◆ 涉及其他信息主体的信息时，宜进行屏蔽展示，当满足如下条件之一时可不脱敏：
    - ■ 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；
    - ■ 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；
    - ■ 其他法律法规要求的情况。

4.3 逻辑安全

4.3.1 逻辑安全设计

移动金融客户端应用软件应满足以下要求：

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).客户端代码实现应尽量避免调用存在安全漏洞的函数，避免敏感数硬编码。

4.3.2 客户端权限最小化

只赋予完成操作的必备权限和最少功能。Android程序本身可以在安装时被授予很多权限和功能，如发送短信、手机定位、访问本机图库等，这些权限和功能在特定环境下可能被恶意代码所利用。

权限仅在使用时才进行声明和获取。

4.3.3 风险控制

a).客户端运行环境的网络环境变化时应有相应的网络切换提示；

b).客户端进入手机后台运行时应有相应的提示；

c).客户端安装后，用户首次打开客户端应有隐私政策和用户协议的对话框提示，并在客户端固定栏目展示隐私政策和用户协议；

d).客户端在获取系统权限时，需要向用户做出提示说明该权限使用的场景；

4.3.4 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。

4.3.5 异常处理

a).客户端发生故障产生的一场信息，不应泄露用户的敏感数据；

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

4.4 安全功能设计

4.4.1 组件安全

a).客户端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。

4.4.2 接口安全

a).客户端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；
b).客户端应对传入的URI进行校验与安全处理，防止客户端运行异常或操作异常；
c).当客户端需要与TEE、SE结合使用时，应避免使用存在已知漏洞的接口。

4.4.3 抗攻击能力

4.4.3.1 源代码保护

Android应用源代码保护要求包括以下方面：
a).对Android程序代码进行混淆保护，防范攻击者对客户端程序的调试、分析和篡改；
b).对Android程序代码使用专业加固软件/服务进行保护，防范攻击者对客户端程序的调试、分析和篡改；
c).对于嵌入客户端中的H5代码、动态下发的小程序或者H5离线包需要进行必要的前端代码混淆，增加对抗中逆向的难度。

4.4.3.2 编译保护

IOS应用开发时必须使用官方的编译软件进行编译，不得从第三方下载。

4.4.3.3 真实性和完整性校验

a).使用企业的证书对客户端进行签名，不发布无数字签名的软件；
b).在与服务器首次通讯时，将签名信息发送至服务器进行签名比对校验，拒绝与签名校验失败的客户端继续通讯；

4.4.4 客户端环境监测

应符合JR/T 019-2020《证券期货业移动互联网应用程序安全规范》，客户端在运行时应具备对运行环境的检查能力，检查的范围可包括：系统是否被未经授权获取管理员权限、程序运行环境是否可信（如：是否运行在模拟器或虚拟机中）等，并能向后台系统反馈设备信息等。

4.5 缺陷解决率

移动客户端缺陷按照严重程度主要分为三个等级：严重缺陷、一般缺陷、轻微缺陷。
a).严重缺陷是指客户端出现崩溃、白屏、闪退、功能流程错误、数据异常、程序接口错误、高危安全漏洞等问题。严重问题缺陷修复率应为100%，且在3个工作日内处理完成；
b).一般缺陷是指功能未实现，界面出现错误、部分机型兼容性问题、数据部分缺失等问题。一般问题缺陷修复率应为95%以上，且在15个工作日内处理完成；
c).轻微缺陷是指界面显示小问题，如错别字、界面不美观、栏目位置不正确、操作不方便等问题。由项目负责人和业务部门协商轻微缺陷修改时限，如确认修改，轻微问题缺陷修复率应为90%以上，且在30个工作日内处理完成；如确认本次不修改，则在下一个版本处理完成。

4.6 数据安全

4.6.1 数据获取

a).客户端保证内存不应存在完整的交易密码、银行卡密码和网络支付密码明文；
b).客户端的临时文件中不应出现交易敏感信息，临时文件包括但不限于Cookies、本地临时文件等；
c).客户端应禁止在身份认证结束后存储交易敏感信息，防止交易敏感信息泄露；
d).客户端运行日志中不应打印交易敏感信息，不应打印完整的交易敏感数据原文；
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；
f).客户端应实现身份认证过程的防截屏、录屏，如：输入手势验证码、登录口令等。

4.6.2 数据访问控制

a).应采取措施保护客户端数据仅能被授权用户或授权应用组件访问；
b).客户端在授权范围内，不应访问非业务必需的文件和数据。

4.6.3 数据存储

客户端在数据存储时，应满足以下要求：
a).客户端不应在客户未许可或不知情的情况下存储客户敏感信息，且不应以任何形式明文存储密码信息；
b).客户端删除后，应清除移动终端中的所有客户信息；
c).客户端退出时，应清除或加密存储客户的敏感数据。

4.6.4 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，客户端在展示个人信息时，如银行账号、身份证号码、手机号码、姓名等时应屏蔽关键字段。

4.7 网络通信安全

4.7.1 客户端与服务器的通信安全

a).应在客户端与服务器之间建立安全的信息传输通道，防止数据在传输过程中被篡改；
b).应确保采用的安全协议不包含已知的公开漏洞；
c).客户端与服务器应进行双向认证，可通过密钥、证书等密码技术手段实现服务器与客户端之间的安全认。

4.7.2 会话失效

客户端在安全退出登录时，应向服务器发送绘画结束请求，使当前会话状态失效。

5 移动金融客户端应用软件管理要求

5.1 设计要求

应符合JR/T 0092-2019《移动金融客户端应用软件安全管理规范》，满足以下要求：
a).客户端设计应遵循安全、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；
b).客户端应提供易用、风格统一、体验良好的用户界面；
c).客户端应遵循合法、正当、必要的原则，不收集与所提供服务无关的个人金融信息；

d).客户端收集个人金融信息或用户授权等操作前，要以通俗易懂、简单明了的方式展示个人金融信息收集使用规则，并经个人金融信息主体自主选择同意；
e).客户端不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反与用户的约定收集使用个人金融信息；
f).客户端应提供访问、更正个人金融信息，以及账户注销等功能。

5.2 开发要求

应符合JR/T 0092-2019《移动金融客户端应用软件安全管理规范》，满足以下要求：
a).客户端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).客户端开发过程中应建立并维护开发文档；
c).客户端开发完成后，应同步完成产品手册、用户手册或提供在线帮助说明；
d).客户端每次重要更新、升级，都必须经过严格源代码扫描、发布审核等步骤。

5.3 开发环境隔离

客户端开发过程中必须进行有效的环境隔离，包括但不限于开发环境、测试环境、仿真环境、生产环境等，有效防止账户在不同环境的混用。

5.4 安全测试

移动金融客户端应用软件应满足以下安全性功能要求：
a).客户端在开发完成，正式上线前，应进行安全测试和安全加固；
b).应提供安全性功能操作文档，应提供安全性功能测试文档。

5.5 发布和更新要求

5.5.1 客户端发布

a).客户端应有规范的上线发布流程，由客户端的所有方对客户端进行签名和保护，标识客户端的来源和发布者，提供安全可靠的客户端下载、发布、升级渠道；
b).正式版本发布时，应删除测试数据和所有用于调试的代码；
c).客户端安装过程中，应拥有独立的安装目录，唯一的应用标识符，明确的版本序号，不得篡改、覆盖、删除系统文件和其他软件。

5.5.2 客户端更新

a).对移动金融客户端应用软件动态安装文件或补丁文件的管理要求，移动客户端应该提供正规的更新渠道，并明确告知客户版本更新内容；
b).移动客户端应该提供灰度更新能力，保障版本更新发布的安全性；
c).客户端更新后应该不影响客户当前版本保存的临时性数据；
d).对于由于监管、合规、技术等原因引发的强制更新，必须提前以明显的方式通知客户。

5.6 兼容性

a).客户端应兼容市面上大多数主流机型，兼容终端数量≥500；
b).客户端应兼容市面上主流的Android和IOS操作系统，做到兼容Android5.0以上、IOS 8.0以上；
c).客户端应兼容HarmonyOS（鸿蒙系统）；

d).客户端支持IPv6访问。

5.7 性能

a).应控制客户端安装包大小，删除无用的第三方SDK、资源文件、类、属性、方法，包括但不限于静态资源包剥离、res资源文件优化、lib优化：

- 静态资源包剥离：将客户端业务静态资源打包剥离并放置到服务器端，安装包内仅保留必要原生资源，安装完成后客户端通过服务器端进行初始化，拉取最新文件资源，且在更新业务内容时，可支持仅更新服务器端静态资源即可完成，无需用户重新下载安装；
- res资源文件优化：尽量使用自适应布局，减少布局文件数量，图片资源经过压缩后进行资源文件集成，删除无用的图片、xml等资源；
- lib优化：避免使用功能重复的lib库，删除无用的lib库。

b).客户端在不同设备上的冷启动时间应小于1秒；

c).客户端后台服务器响应时间应小于1秒；

d).客户端核心服务器并发量经过压力测试，达到以下标准：

交易服务，单台服务器支持并发数1000以上；

接入服务，单台服务器支持并发数1000以上；

e).CPU占有率要求：

空闲时段（切换到后台），CPU占有率小于10%；

高负荷运行峰值，CPU占有率小于35%；

f).内存占有率要求：

空闲时段（切换到后台），内存占有率小于5%；

高负荷运行峰值，内存占有率小于25%；

5.8 软件共存

移动金融客户端应用软件需要保证与其它独立移动客户端软件的共存性。

a).在安装时，不能存在因其它独立移动客户端软件影响而无法安装的情况；

b).在运行时，不能存在因其它独立移动客户端软件影响而功能无法正常使用的情况。

5.9 维护要求

应符合JR/T 0092-2019《移动金融客户端应用软件应用软件安全管理规范》，满足以下要求：

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).以SDK等形式对外提供金融交易类服务时，应记录SDK信息及引用本SDK的外部应用软件信息。

5.10 安全审计

5.10.1 日志生成

应符合JR/T 019-2020《证券期货业移动互联网应用程序安全规范》，满足以下要求：

a).日志应包括事件发生的日期、时间、用户标识、设备唯一标识、设备型号、设备版本、网络类型、事件描述和结果等信息；

b).日志应该如实记录用户各项重要操作，如用户登录成功和失败；校验失败的次数超出阀值导致会话连接终止等；
c).正式发布的移动终端程序不能包含调试过程中的日志。

5.10.2 日志管理

应符合JR/T 019-2020《证券期货业移动互联网应用程序安全规范》，满足以下要求：
a).日志应存储于掉电非易失性存储介质中；
b).仅允许授权用户以只读形式访问日志，且支持日志审计；
c).日志应具备查询功能；
d).日志不应记录客户敏感信息；
e).日志应存放于服务器端；
f).日志保存的时间不少于十二个月，满足业务管理、审计、监督检查等需要。

5.11 创新及前瞻性

5.11.1 无障碍服务

a).客户端可提供字体大小调整功能，行情数据显示字体可进行小、中、大、特大调整，资讯内容字体可适当放大，调整后不影响整体效果；
b).客户端可进行换肤，以便适应不同环境下客户端的显示效果；
c).部分页面支持利用手势进行页面文字及图片的缩放。

5.11.2 生物识别

a).客户端Android交易登录支持指纹特征识别,错误拒绝率小于等于3%，错误接受率小于等于0.001%；
b).客户端IOS交易登录支持指纹特征识别,错误拒绝率小于等于5%，错误接受率小于等于0.01%。

5.11.3 视频服务

a).采用高强度AES+独家密码本混淆加密技术，通过对视频进行逐帧加密，杜绝被破解下载，同时搭配防翻录、防盗播和防篡改功能，可实现从视频源、传播途径、播放终端的全方位技术防御；
b).可实现视频画面预加载，弱网环境也可首屏快速打开，支持多码率和多倍速播放

5.11.4 IM智能在线客服

a).应支持自然语言交互实现用户意图识别和知识答案ID解析；
b).服务提供时间应实现7*24小时服务；
c).应支持全渠道触达，可覆盖APP、网站、微信、小程序等；
d).在线客服功能场景覆盖公司业务场景不小于90%。

参考文献

[1] JR/T 0092-2019《移动金融客户端应用软件应用软件安全管理规范》
[2] JR/T 0192-2020《证券期货业移动互联网应用程序安全规范》
[3] JR/T 0171-2020《个人金融信息保护技术规范》
[4] JR/T 0191-2020《证券期货业软件测试指南软件安全测试》