Q/DBZQ

东北证券股份有限公司企业标准

Q/DBZQ 001-2023

移动客户端应用软件开发规范

2023-01-01 发布

2023-01-01 实施

东北证券股份有限公司 发布

目 次

1 范围	4
2 规范性引用文件	4
3 术语和定义	4
4 缩略语	5
5 移动客户端应用软件技术规范	5
5.1 兼容性	6
5.2 性能	6
5.3 稳定性	6
5.4 会话机制	6
5.5 版本更新	7
5.6 三方 SDK 管理	7
5.7 生物特征	7
5.8 多站点和 CDN	8
5.9 无障碍	8
5.10 共存性	8
6 移动客户端应用软件安全规范	8
6.1 应用程序	8
6.2 运行环境	9
6.3 身份认证	9
6.4 密码	9
6.5 网络通信	9
6.6 数据存储	10
6.7 个人信息保护	10
7 移动客户端应用软件质量管理规范	10
7.1 需求分析阶段	10
7.2 架构设计与开发阶段	11
7.3 测试阶段	11
7.4 发布阶段	12
7.5 运行阶段	13
参考文献	13

前 言

本标准按照 GB/T 1.1-2022 《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本标准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。

本标准由东北证券股份有限公司提出并归口。

本标准起草单位：东北证券股份有限公司。

本标准主要起草人：金华、李继骏、张金鑫、张泽鑫、郑飞飞、邱晶良、袁廷建、董尚阳、蒙永钢。

本标准为首次发布。

移动客户端应用程序研发规范

1 范围

本标准规定了东北证券股份有限公司移动客户端软件技术规范、安全规范以及软件质量管理等要求。

本标准适用于东北证券股份有限公司移动客户端应用程序的设计、开发、测试、发布和维护过程，也适用于主管监管部门、第三方评估机构对相关应用进行安全性和标准符合性的评估。

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 37668-2019 信息技术 互联网内容无障碍可访问性技术要求与测试方法

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

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 0092—2019 移动金融客户端应用程序安全管理规范

JR/T 0191—2020 证券期货业软件测试指南 软件安全测试

3 术语和定义

下列术语和定义适用于本文件。

移动客户端应用程序 **mobile application software**

在移动终端上为用户提供服务的应用软件。

注：包括但不限于可执行文件、组件等。

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。

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：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。

指纹识别 fingerprint recognition

以人手指指纹作为识别个体身份的一种个人生物特征识别方法。

人脸识别 face recognition

以人面部特征作为识别个体身份的一种个人生物特征识别方法。其通过分析提取用户人脸图像数字特征产生样本特征序列，并将该样本特征序列与已存储的模板特征序列进行比对，用于识别用户身份。

注：从应用方式不同，人脸识别可分为人脸验证和人脸辨识。

代码评审 source code review

是指通过阅读代码来检查源代码与编码标准的符合性以及代码质量的活动。

代码混淆 source code obfuscation

是将计算机程序的源代码转换成难于阅读和理解的形式行为。

签名 signature

包含有公钥的公钥证书。其中的公钥用来认证数字签名，而不能加密数据或执行其他的密码功能。

会话 Session

一个终端用户与交互系统进行通讯的过程。

动态调试 Dynamic debugging

破解者利用调试器跟踪软件的运行，寻求破解的途径。

4 缩略语

下列缩略语适用于本文件。

APP: 客户端应用软件 (Application software)

SDK: 软件开发工具包 (Software Development Kit)

IP: 网际互连协议 (Internet Protocol)

CDN: 内容分发网络 (Content Delivery Network)

5 移动客户端应用软件技术规范

5.1 兼容性

移动客户端应用软件需满足不同设备多系统版本下都能正常运行，应具备以下兼容性要求：

1. 支持主流软件系统：Android、iOS 和 HarmonyOS (鸿蒙)；
2. 最低支持 Android 4.4 系统版本、iOS 9.0 系统版本和 HarmonyOS 全部系统版本；
3. 对主流移动设备、屏幕分辨率均能提供稳定的支持，每个版本发布前使用兼容性测试平台对主流机型进行深度兼容测试；
4. 对主流折叠屏或平板类设备提供主体功能的正常使用；
5. 对三大运营商网络环境均能提供流畅的功能体验，同时支持 IPv4 和 IPv6；
6. 在弱网和网络切换场景下都能正常使用，对无网环境进行相应提示；
7. 依据主流应用市场要求，Android 版应全面支持 64 位应用，对有特殊要求的应用市场和用户可提供 32 位兼容版本，iOS 版根据 App Store 要求支持 iPhone 5s 之后的设备。

5.2 性能

1. 移动客户端应用软件应控制安装包大小处于合理范围，方便客户快速下载使用和避免对客户流量消耗过大，安装包大小(除第三方 SDK 以外)不大于 60M；

2. 移动客户端应用软件应建立统一的安装包大小优化机制，可从删除无用资源、res 资源文件压缩、图片压缩、同类型库不得重复引入、无需支持的 CPU ABI 架构删除、开启混淆压缩等方面优化；

3. 移动客户端应用软件冷启动时间（Android 不含解壳时间）在主流移动设备上应控制在 1 秒以内；在网络情况良好的状态下，使用网络请求的业务功能响应时间应控制在平均值 1 秒以内；

4. 移动客户端应用软件后台服务器对交易类核心功能应提供不低于每秒 10 万的并发量；其他业务不得低于每秒 5000 的并发量；

5. 移动客户端应用软件功能压测应进行日常真实吞吐量和并发量 5 倍数据量场景的验证。

5.3 稳定性

移动客户端应用软件开发应满足稳定性方面的要求，应在开发、测试阶段完成闪退、卡顿、内存泄露等问题的开发自查和集成测试，相关自查、测试标准如下：

1. 研发团队应有编写单元测试用例的技术方案和用工具检测客户端闪退、卡顿、内存泄漏的客户端检测机制，并在提交测试前完成稳定性方面开发自查；

2. 应通过自动化真实用户感知系统，持续监测线上版本运行的稳定性。

5.4 会话机制

1. 移动客户端应用软件应有统一的会话管理机制；

2. 移动客户端应用软件应区分非交易和交易会话在线状态，非交易会话可保持较长时间在线状态，交易会话应默认保持 5 分钟在线状态，用户可设定交易会话保持在线时间，最低 5 分钟，最高 2 小时，超出时间应踢出交易登录态；

3. 用户从移动客户端应用软件登出后，服务端应同步登出，不得出现被抓取报文重放等现象。

5.5 版本更新

移动客户端应用软件支持应用内版本检测和更新功能，秉持稳健运行原则，应满足如下要求：

1. 支持按照版本号提示升级和强制升级，原则上每个版本要做好对历史版本的兼容，非必要不使用强制升级功能；

2. 正式版本应关闭调试、日志打印等功能；

3. 正式版发布应用市场前，应进行灰度验证和分阶段发布，避免出现较大范围问题。

5.6 三方 SDK 管理

移动客户端应用软件研发流程应建立统一的组件化工程结构，通过统一的框架对自有开发组件和三方 SDK 进行版本管理，有效的控制三方 SDK 集成接入软件的风险：

1. 三方 SDK 接入前，应进行授权管理、开源协议、SDK 安全检测、隐私合规评估等事项；

2. 移动客户端应用软件应避免使用存在已知漏洞的组件和三方 SDK，并定期进行代码漏洞扫描和应用安全测评；

3. 测试阶段应对接入的三方 SDK 进行全面测试，并对三方 SDK 的兼容性、稳定性、安全性、个人信息保护和其他法律合规性的影响进行分析，符合要求的才进入发布阶段；

4. 三方 SDK 升级必要性应有明确的判断标准，不得随意进行三方 SDK 升级；

5. 进行三方 SDK 升级时应与第三方进行升级内容和影响范围确认，保证三方 SDK 升级稳定；

6. 三方 SDK 进行新接入和升级后，应对整个 APP 进行充分测试，避免影响其他功能模块。

5.7 生物特征

移动客户端应用软件采用生物特征识别技术进行身份认证功能，能提高用户使用体验，Android 版通常采用指纹特征识别技术，iOS 版通常采用人脸特征识别技术。移动客户端应用软件生物特征识别应满足如下要求：

1. 指纹、人脸识别等生物特征应只是业务安全性验证中的一个环节，不能把生物特征作为仅有的技术验证手段，如可结合短信验证码等其他方式共同验证；

2. 应根据运行设备的硬件条件选择采用指纹或人脸特征识别。

5.8 多站点和 CDN

1. 移动客户端应用软件应支持多站点服务器，多站点服务器可提高服务器的可靠性、性能和安全性，适用于对网络性能和可用性有要求的场景，如股票行情实时数据更新；

2. 移动客户端应用软件应支持 CDN，CDN 能解决跨地域跨运营商网络性能问题，提供稳定快速的加速服务，如静态内容分发。

5.9 无障碍

移动客户端应用软件应提供多种无障碍服务功能，如支持以下功能：

1. 支持日间和夜间版本皮肤；
2. 支持行情正常字号版和大字号版；
3. 支持普通版、长辈版等多种模式；
4. 在资讯浏览页面，提供调节字体大小功能；
5. 在某些场景支持语音输入；
6. 应满足 GB/T 37668-2019《信息技术 互联网内容无障碍可访问性技术要求与测试方法》中所有三级要求。

5.10 共存性

移动客户端应用软件运行的终端设备存在多个不同类别 APP 共享设备资源的场景，共存性要求应满足如下：

1. 安装或运行 APP 时不与设备上的其他 APP 发生冲突；
2. 不与系统内置软件、系统安全软件发生冲突。

6 移动客户端应用软件安全规范

6.1 应用程序

参照 JR/T 0192—2020《证券期货业移动互联网应用程序安全规范》，移动客户端应用软件应采取防动态调试、代码混淆、防逆向等技术对关键代码、核心逻辑进行保护，具体要求如下：

1. 移动客户端应用软件应使用企业证书进行签名，不发布无签名的软件；
2. 移动客户端应用软件应采用防逆向保护措施，包括代码混淆、安全加固等；
3. 移动客户端应用软件启动时应进行应用签名校验，防止被反编译后进行二次打包；
4. 移动客户端应用软件应有防止 Cycript 等动态调试框架的检测，避免运行时的被动动态调试。

6.2 运行环境

参照 JR/T 0192—2020《证券期货业移动互联网应用程序安全规范》，移动客户端应用软件应在每次运行前对运行环境的安全性进行检测，并提示发现的风险，具体要求如下：

1. 移动客户端应用软件 Android 版应限制在 root 环境和模拟器环境下使用，iOS 版应限制在越狱环境下使用；
2. 移动客户端应用软件应检测运行环境是否存在网络代理，并进行必要的安全提示；
3. 移动客户端应用软件在检测到客户终端设备处于不安全环境时，应实时反馈安全状况到后台系统；
4. 当移动客户端应用软件切换到手机多任务预览窗口时内容应模糊展示。

6.3 身份认证

1. 认证方式应提供密码、短信验证码、生物特征识别、图形验证码、手势密码等多种方式；

2. 应限定连续登录失败次数，如登录失败次数达到上限时应限制用户登录行为；

3. 当长时间无操作导致会话超时登出后，应重新进行身份认证才能继续操作；

4. 应加强人脸识别技术在身份认证中的安全方案，具备人脸识别图片防篡改功能，切实消除人脸识别技术的安全风险隐患。

6.4 密码

移动客户端应用软件密码安全性应满足如下要求：

1. 密码不应以任何形式明文保存在移动终端的本地存储上；

2. 密码在传输过程中必须加密传输，采用国密算法加密；

3. 密码输入框默认不得为明文显示模式；

4. 密码输入时键盘应使用安全键盘，支持随机键位，不得被工具监听；

5. 密码信息不得在日志或缓存中打印输出；

6. 应用程序应对密码（包括登录密码、交易密码）、银行卡号等敏感信息进行加密；

7. 修改密码时应对用户进行身份校验，新密码不能与旧密码相同；

8. 密码设置应满足一定的复杂度要求；

9. 密码输入等页面应对录屏截屏行为进行提示或限制，且密码输入键盘不得有键位点击效果；

10. 密码输入页面切到后台后，应及时清理密码输入框密码内容。

6.5 网络通信

1. 移动客户端应用软件应对通信报文进行加密，防止敏感数据泄露，加密算法应使用

国密算法；

2. 移动客户端应用软件应对通信报文进行签名，防止数据在传输过程中被篡改；
3. 应对通信报文进行时间戳校验，有效避免重放攻击。

6.6 数据存储

1. 移动客户端应用软件应仅保存业务必须的个人金融信息，并限制数据存储量，对用户敏感信息必须加密保存；
2. 移动客户端应用软件不得以任何形式存储用户支付敏感信息、用户口令等数据；
3. 移动客户端应用软件存储应不能被其他应用访问；
4. 移动客户端应用软件在会话结束后应立即清除敏感数据缓存，防止信息泄露；
5. 移动客户端应用软件在应用软件被卸载后，文件系统中不应残留任何个人金融信息。

6.7 个人信息保护

移动客户端应用软件在个人信息保护方面应满足如下要求：

1. 在用户冷启动 APP 时，要提醒用户阅读 APP 隐私政策（包含首次打开 APP 和打开 APP 发现有隐私政策更新），在用户未同意隐私政策之前不得进行任何形式的个人信息收集行为；
2. 权限申请应遵循最小必要原则，与业务场景无关权限不进行声明，在用户申请权限时应明确告知权限描述、使用场景等信息；
3. 移动客户端应用软件不得使用自启动和应用保活等技术，要求第三方 SDK 不得使用关联启动技术；
4. 移动客户端应用软件各项业务不得超出隐私政策范围去收集个人信息，隐私政策应向用户明示收集个人信息的目的、类型、使用场景；
5. 移动客户端应用软件应能够保障输入信息的机密性，如采取自定义键盘、随机键盘位、防范键盘窃听技术等措施；
6. 移动客户端应用软件不应在客户未许可或不知情的情况下存储个人敏感信息，且不应以任何形式存储明文密码信息；
7. 隐私政策应对用户提供同意撤回功能；
8. 移动客户端应用软件应满足 GB/T 35273-2020《信息安全技术 个人信息安全规范》和 JR/T 0171—2020《个人金融信息保护技术规范》规范要求。

7 移动客户端应用软件质量管理规范

7.1 需求分析阶段

1. 每个业务需求都需要进行需求评审，评审通过后才能实施开发。需求评审会由项目经理发起，参会人员包括产品经理、开发工程师、测试工程师以及其他项目成员。评审会上由产品经理对需求内容进行澄清，说明需求背景、需求内容、价值分析与期望；参会人员需求质量进行把关，评估需求完整性、合理性及技术可行性，并决定评审结果。

2. 需求评审通过后，由项目经理牵头需求分析并编写需求分析结果文件，参会人员包括系统架构师、开发工程师、产品经理；需求分析的内容包括但不限于分析技术可行性、埋点分析、IT 规划一致性、成本风险、存在的困难、系统异常情况兜底方案、对上下游的影响、优先级、预估用时、预估上线排期、并填写需求分析结果文档。

7.2 架构设计与开发阶段

1. 需求分析完成后，需进行架构设计。架构设计由系统架构师负责，项目经理、核心开发工程师参与；架构设计内容包括但不限于接口设计、数据库设计、系统健壮性、可扩展性、系统性能、安全性、第三方数据或者接口的可靠性判断、是否符合公司规划、是否符合项目系统架构规划等因素，并形成设计文档。

2. 各系统要做好代码分支管理，每个系统至少包含 4 个代码分支，分别为开发分支 `nesc_dev`、测试分支 `nesc_test`、通关分支 `nesc_release`、主分支 `nesc_master`，每个版本新建版本分支，每个需求新建 `feature` 分支。

3. 代码仓库和代码分支管理具体要求包括：

(1) 所有代码仓库应设置为私有，具备权限分配、代码查看、代码合并、分支管理等功能；

(2) 代码仓库需要设置管理员，管理员对主要分支进行代码评审，设置权限等；

(3) 主干分支和版本分支应设置为受保护分支，仅代码仓库管理员可推送更新至受保护分支；

(4) 开发者向代码仓库提交代码时，代码仓库管理平台应执行统一的编码规范检查，拒绝不符合编码规范的代码变更，同时还需要进行人工代码审查。

4. 开发工程师须按照编码规范编写代码，开发过程中须考虑函数、逻辑、技术选型的合理性与性能等。开发工程师须对代码进行自测，自测通过后才能提交测试，开发工程师对自己编写的代码负责。

5. 系统架构师须对每一个版本的代码进行审查，按照代码审查规范审核代码。

6. 编码完成后，系统架构师负责提供测试安装包，测试安装包包括但不限于本版本的所有增量代码文件、数据库变更脚本、配置文档、其他修改项、单元测试报告、提测的需求单列表、每个 Jira 的影响范围、部署注意事项、升级说明，并确保与版本需求范围保持一致，严禁夹带。

7.3 测试阶段

1. 测试工程师负责编写测试方案并组织评审，参与人员包括项目经理、产品经理、架构师、开发工程师、测试工程师、信息安全工程师，测试方案内容包括但不限于功能测试范围、兼容性测试范围、测试机型、测试计划、人员分工。

2. 测试工程师负责编写测试用例并组织评审，参会人员包含项目经理、产品经理、开发工程师，测试用例评审通过后执行。测试用例的编写需充分考虑功能覆盖度、异常场景、边界值情况等。同时，根据实际情况分级和维护多套测试用例，包括但不限于完整的测试用例、冒烟级别用例、核心功能用例。

3. 测试工程师须提前根据测试用例准备测试数据，开发工程师、运维人员以及其他人员配合。

4. 版本提测后，测试工程师首先进行冒烟测试，冒烟测试主要包括对相关文档的审核、环境连通性测试、主功能可用性测试等。若冒烟测试不通过，则拒绝准入测试，项目经理重新组织开发人员修改并提供新的测试安装包，直至冒烟测试通过。

5. 冒烟测试通过后，开始功能测试，测试工程师根据测试计划执行测试用例，确保执行每条测试用例；测试过程中思考需求设计合理性、测试点错漏。

6. 除功能测试外，每个版本都需要做自动化测试，作为功能测试的补充。原生客户端变更必须做全量回归测试，H5 或服务端变更可根据情况确定是否需要做自动化测试。

7. 每个版本还需进行兼容性测试，若版本涉及原生客户端变更或者核心功能变更则必须做兼容性测试，测试内容包括但不限于交易核心功能、重要新功能。

8. 版本更新或新上线均需通过应用安全测评，服务器端需通过漏洞扫描、基线核查的等安全检测，对于中、高危漏洞须修复后方可上线。

9. 对于有新增接口或影响性能的版本，还需要做压力测试并输出压力测试报告，对于压力测试结果不符合要求的，需进行整改，通过后才能上线。

10. 测试通过后，测试工程师负责编写测试报告并组织评审，参会人员包括项目经理、产品经理以及相关人员。测试报告内容包括但不限于测试范围、回归测试范围、测试机型、质量评估、可靠性评估、兼容性评估、性能评估、安全评估、遗留问题、关键风险、测试结论。

11. 需求部门进行验收测试，包括测试环境验收测试和生产环境验收测试，并提供验收测试报告。

12. 版本上线前，需编写上线确认单，项目经理负责上线确认单发起，系统架构师、开发工程师、测试工程师配合完成上线确认单。上线确认单的检查通过对比上一版本代码的形式来进行，检查项包括但不限于程序包是否有夹带、上线需求是否与版本需求清单一致、配置、版本号、服务器地址、SDK 是否生产环境、均衡功能、交易登录买卖测查功能、推送、加固签名，上线确认单的检查项需要截图。

13. 在正式发布生产环境前，需进行通关测试，项目经理负责通关测试流程以及相关环境要素准备，运维人员负责通关部署通关测试环境。

14. 每个系统至少包含 4 套环境，1 套开发环境、2 套测试环境、1 套仿真环境，开发工程师负责开发环境搭建、管理以及发布工作，测试工程师负责测试环境和仿真环境的搭建、管理以及发布工作，仿真环境应与生产环境保持架构一致，且定期脱敏同步数据。

7.4 发布阶段

1. 项目经理负责升级计划文档编写并组织会议评审，运维人员、系统架构师、开发工程师以及相关人员进行；升级计划包括但不限于每个系统的发布内容、发布顺序、发布时间、是否依赖第三方、网络策略、增加硬件、开发负责人以及注意事项。

2. 版本发布前项目经理通知相关系统或模块的负责人，防止关联系统升级计划变更导致版本回退情况。

3. 需进行灰度发布，灰度时间通常为一周，灰度发布完成后方可进行全量发布。

4. 每次发布后都需要业务盘检，保证每台服务器都已发布最新程序版本。

7.5 运行阶段

1. 灰度发布期间属于试运行阶段，试运行期间需及时跟踪运行情况，发现问题后由项目经理及时通知相关方并处理。

2. 需进行日常业务盘检，每个交易日检查两次，8点半之前检查一次，9点15分之前检查一次；法定节假日前一天检查一次。

3. 生产事故形成事故报告并留档，便于后续统计，事故报告内容包括但不限于事故描述、根本原因、影响、临时解决方案以及完成时间、长期解决方案以及完成时间。

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 37668-2019 信息技术 互联网内容无障碍可访问性技术要求与测试方法

[3] GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

[4] JR/T 0171—2020 个人金融信息保护技术规范

[5] JR/T 0192—2020 证券期货业移动互联网应用程序安全规范

[6] JR/T 0092—2019 移动金融客户端应用软件安全管理规范

[7] JR/T 0191—2020 证券期货业软件测试指南 软件安全测试

[8] 工信部 191 号文 APP 违法违规收集使用个人信息行为认定方法