ICS 35.240.40
A 11

Q/GXNX

广 西 农 村 信 用 社 企 业 标 准

Q/GXNX 003—2020

移动金融客户端应用软件服务企业标准

GUANGXI RURAL CREDIT UNION

Enterprise Standard for Financial Mobile Application Software

2020 - 09 - 30 发布　　2020 - 10 - 30 实施

广西壮族自治区农村信用社联合社发布

目　　录

前　言

本标准按照GB/T 1.1 2009给出的规则起草。

本标准由广西壮族自治区农村信用社联合社提出。

本标准由广西壮族自治区农村信用社联合社电子银行部归口。

本标准起草单位：广西壮族自治区农村信用社联合社电子银行部、计算机网络中心。

本标准主要起草人：刘剑、郑胜前、劳谦、何妹、战韦达。

本标准为首次制定。

引　言

近年来，随着技术和社会的不断发展和变革，用户对移动金融客户端应用软件安全和体验的要求也不断提高，由此对移动金融产品设计开发工作规范化提出了更高要求。为进一步明确移动金融产品的设计原则、安全要求、技术先进性、创新及前瞻性等，特制订本标准。

广西农村信用社移动金融客户端应用软件服务企业标准

1 范围

本标准规定了广西壮族自治区农村信用社（农村商业银行、农村合作银行）的移动金融客户端应用软件的设计原则、安全要求、技术先进性要求、创新及前瞻性目标，适用于移动端金融产品方案设计、需求编写、页面设计、技术开发和产品测试环节，用于指导需求编写、系统设计开发等工作。

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。

GB/T 25069-2010 信息安全技术术语

GB/T 35273-2017 信息安全技术个人信息安全规范

JR/T 0068-2020 网上银行系统信息安全通用规范

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

下列术语和定义适用于本文件。

3.1

移动金融客户端应用软件 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：包括但不限于可执行文件、组件等。

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1：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。

注2：改写 GB/T 35273—2017，定义 3.1。

3.3

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。

3.4

语音识别 automatic speech recognition

将人类语音中的词汇内容转换为计算机可读的输入。

示例：按键、二进制编码或者字符序列。

3.5

自然语言理解 natural language processing

使用自然语言同计算机进行通讯的技术。

4 符号和缩略语

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)

Session：当用户使用客户端应用软件时，服务器端会给用户创建一个独立的 Session（会话）

OCR：图像识别（Oprical Character Recognition）

GC：垃圾回收机制（Garbage Collection）

UI：用户界面（User Interface）

root: 针对 Android 系统的手机而言，它使得用户可以获取 Android 操作系统的超级用户权限。

5 设计要求

5.1.1 页面风格

5.1.1.1 布局均衡

a) 可通过应用栅格化工具，建立参考线，使界面布局整洁有序。
b) 可通过界面元素对齐、排列，体现视觉元素的秩序性。
c) 可运用界面元素间大小、色彩、位置对比，体现视觉平衡感。
d) 应合理分配界面元素间的距离，形成均衡的视觉感受。

5.1.1.2 配色和谐

应通过搭配合理的色彩对比（明度、纯度、色相）带来的和谐视觉感受。可使用明度高的色彩传达出便捷、灵活的视觉感受，使用明度低的色彩传达出沉稳、专业的视觉感受。

5.1.1.3 元素简洁

a) 应避免在界面设计时使用过分的装饰元素和种类过多的色彩。
b) 应通过平衡重心视觉布局呈现界面信息，使界面设计中重点内容突出。

5.1.2 便捷性

5.1.2.1 流程连贯

a) 应合理规划界面顺序，避免流程中的折返。
b) 应根据用户习惯，为用户推荐常用的功能入口。

5.1.2.2 输入简化

a) 应通过直接操作界面元素来提升操作效率。
b) 应减少用户需要输入的要素信息。
c) 应用尽量使用选择的方式代替键盘输入。
d) 应为用户推荐合理的默认值及其他方式来简化用户的操作复杂度，提升操作效率。

5.1.2.3 反馈友好

a) 应在用户输入过程中进行关联提示。
b) 应利用突显色彩效果表达系统及页面元素增减、页面间变化。
c) 应对用户的任务进度进行提示。

5.1.3 容错性

a) 应在用户进行录入和选择操作时，及时校验用户录入的信息，并给予相应提示，以提高用户输入的准确性。
b) 应在用户进行有风险操作时，提供二次确认。
c) 应在用户完成任务时，结合实际需求为用户提供撤销操作的功能，以避免用户因操作失误而导致错误的发生。

5.1.4 架构设计合理

a) 应根据产品的设计目标，实现使产品信息层级扁平化。
b) 应根据用户的需求和场景对信息进行分类。
c) 应通过清晰的导航表现产品功能架构，使用户更容易发现所需要的内容和功能。
a) 应采用模块化、组件化设计思想，便于业务拓展与功能扩展。

6 开发要求

a) 客户端应用软件功能开发过程应遵循质量保证、质量控制规则。
b) 应对客户端应用软件功能开发过程遵循安全管理策略、安全设计规范、安全审计原则。
c) 客户端应用软件集成的安全产品，应符合监管部门的有关规定。
d) 应制定客户端应用软件交付清单，并对交付产品进行相应评审。
e) 应制定客户端应用软件开发编码规范，定期进行代码审查，软件交付前应进行代码安全扫描。
f) 应对客户端应用软件进行严格的版本管理，原则上需配置开发库、测试库、产品库，禁止将开发测试版本直接投入产品库中。

7 安全要求

7.1 基本要求

a) 应满足 JR/T 0092-2019 中的基本要求。
b) 应满足 JR/T 0171-2020 中的基本要求。
c) 应满足 GB/T 35273-2017 中的基本要求。

7.2 逻辑安全

7.2.1 逻辑安全设计

a) 在系统进行灰度发布或设置白名单等特殊规则时，应进行严格审查，避免出现逻辑漏洞，导致非授权访问。
b) 在进行逻辑设计时应充分考虑交易流程的合理性，避免出现绕过、重放某些过程步骤，以及改变业务信息流的次序、时序、流向等情况，影响功能交易完整性。

7.2.2 软件权限控制

客户端应用软件申请使用系统权限时，需要明确告知用户授权使用的目的，并得到用户自主授权同意。

7.2.3 风险控制

a) 客户端软件可采取设备认证措施，规避设备更换引起的风险。当用户发生设备变更，需要重新绑定到新设备才能正常使用。
b) 涉及资金交易时应满足以下要求：
   1) 应采取多重维度认证方式，在用户个人信息、口令等部分信息泄漏的情况下，仍能避免用户资金发生损失。
   2) 移动金融客户端软件应建立签约机制及限额控制机制,用户可自行在系统最大限额范围内设定交易额度。
   3) 客户端软件应具备用户自主规避风险的功能。提供用户开通/关闭海外支付功能；提供开通/关闭小额免密支付功能；提供用户挂失/解挂卡等功能。

7.2.4 回退处理

a) 对于未达账的预约转账交易，客户端应用软件提供撤销回退机制。
b) 对于系统异常的转账交易，系统自动回退处理，并提示用户已回退。
c) 对于系统异常确实无法自动回退的情况，应建立相应的人工处理机制进行处理。

7.2.5 异常处理

a) 使用客户端应用软件进行交易过程出现故障或者异常情况时，应通过弹窗等形式提示用户，并停止进行下一步操作。
b) 对于不同类型的异常情况，应满足如下处理要求：
   1) 属于业务完整性缺陷的异常，应提示用户具体原因，用户修正业务信息后，重新发起。
   2) 属于系统故障异常，应提示用户请稍后再试，提示语避免使用难以理解的技术术语。
   3) 属于合规性异常，应提示用户不合规的原因。

7.3 安全功能设计

7.3.1 接口安全

a) 接口调用时应检查请求 Session 是否合法，数据加解密是否通过，防止非法的客户端请求。
b) 应采取措施对客户端应用软件接口进行保护，防止非法调用等行为。

7.3.2 抗攻击能力

a) 采用技术措施，防止手机病毒窃取输入密码动作和事件等。
b) 应保证客户端应用软件自身的安全性，避免代码注入、缓冲区溢出、非法提权等漏洞。

c) 应对客户端程序接口进行源代码安全审查、渗透测试等技术检查，及时处理安全漏洞，有效控制安全风险。

7.3.3 组件安全

对第三方组件、SDK 的使用进行评估，在使用前应进行相应的安全检测。

7.3.4 客户端应用软件环境检测

a) 应对客户端应用软件安装、启动、更新时自身的完整性和真实性进行校验。对客户端运行的环境进行完整性校验，对环境是否进行越狱、root 进行检查。
b) 客户端应用软件应实时检测运行环境，若发现客户端应用软件运行在模拟器环境，则弹出警告信息并自动退出，防止通过各类模拟器运行的攻击手段。
c) 对客户端应用软件的资源文件及配置文件进行完整性校验，防止盗版使用，防止被篡改。

7.4 数据安全

7.4.1 数据获取

7.4.1.1 数据防窃取

a) 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。
b) 资金交易类应满足以下要求：
   1) 客户端应用软件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。
   2) 敏感数据及账号密码等信息，需通过技术手段进行保护，禁止明文存储和直接访问。

7.4.1.2 数据防篡改

a) 采用终端加密、数字签名等技术手段防范数据遭受篡改，防范用户信息在传输过程中被篡改。
b) 客户端应用软件监控内存和进程状态，若检测到内存数据被修改时，则自动退出程序。

7.4.1.3 数据有效性

a) 客户端应用软件应对用户录入的数据进行有效性检查，校验数据格式、长度等，避免因录入非法字符，导致系统处理异常。
b) 客户端应用软件录入敏感信息时，应禁止使用复制、粘贴方式进行录入，避免绕过数据有效性检查。

7.4.2 数据访问控制

客户端应用软件应做好资源文件、配置文件、日志文件等文件的访问控制，防止非法访问。

7.4.3 数据传输

7.4.3.1 通讯安全

应不限于使用防火墙、入侵检测、流量检测、完整性保护系统、防病毒网关等安全产品和安全技术，保障客户端应用软件与服务器之间网络通讯环境安全。

7.4.3.2 数据保密性

a) 客户端应用软件在向服务器传输交易数据前，应支持使用一次性密码对交易数据进行更高强度的加密。
b) 客户端应用软件与服务器端之间，应建立可信安全的加密通道，保证通信过程的可靠性和保密性。

7.4.3.3 数据完整性

客户端应用软件应在用户发起交易请求时，对用户提交的业务信息进行完整性检查，并采取措施对的数据进行完整性保护。

7.4.3.4 数据抗抵赖

a) 客户端应用软件可以采用数字签名技术确保交易请求的不可抵赖性。
b) 客户端应用软件可通过采集设备特征信息、短信验证码、生物识别等手段，增强客户端发起的交易请求不可抵赖性。

7.4.3.5 数据防重放

客户端应用软件向服务端发起交易时，应对每一次传递的交易数据设置唯一标识，服务端应鉴别数据的唯一性，防止遭受重放攻击。

7.4.4 数据存储

a) 客户端应用软件在数据使用完闭后，及时销毁过程数据。
b) 客户端应用软件产生的日志文件、相关过程文件等，不应存储客户个人信息。

7.4.5 数据销毁

7.4.5.1 残余信息保护

保证客户端应用软件无法通过技术手段恢复已被清除的敏感数据。

7.4.5.2 页面返回保护

涉及资金交易的客户端软件应满足以下要求：

a) 客户端应用软件应对后台任务列表中的预览界面采取模糊或其他防护措施。
b) 客户端应用软件从前台进入后台时，超过设定时限后清除页面中已输入的敏感数据，并自动登出。

7.4.5.3 会话失效

a) 客户端应用软件超过规定时间未有任何有效操作，应置会话状态为失效，需要重新建立会话。
b) 客户端应用软件遭受强制退出时，应置会话状态为失效，需要重新建立会话。

7.5 密码算法及密钥管理

7.5.1 密码算法

a) 使用的密码产品应符合国家相关规定，符合监管部门相关要求。
b) 使用密码算法时应优先使用 SM 系列算法。

7.5.2 密钥管理

a) 应采取加密技术等措施来有效保护密钥，避免密钥被非法修改和破坏。
b) 应对生成、存储和归档保存密钥的设备采取物理保护。
c) 应当明确密钥的生存期，使之只在生存期内有效。
d) 客户端应用软件使用不同的工作密钥进行加密时，应保证加密密钥随机性和不可预测性。

7.6 身份认证

7.6.1 身份认证安全

a) 移动金融客户端软件在进行客户身份认证时，应采用两种或两种以上的维度对用户身份进行认证。
b) 在用户身份认证后，客户端应用软件进入终端系统后台时，如果超过设定时限后被唤醒切换到前台，应对用户身份重新认证。

7.6.2 个人信息保护

a) 应采取措施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，不收集与所提供服务无关的个人金融信息。
b) 应采取有效措施保护个人信息，防止数据遭到未经授权的访问、公开披露、使用、修改、损坏或丢失。

7.6.3 安全输入

a) 客户端应用软件使用的第三方安全键盘，应具备有检测资质机构颁发的安全认证证书。
b) 客户端应用软件提供用户输入敏感信息的即时防护功能，防止在录入时被窃取。

7.6.4 个人金融信息展示

移动金融客户端应用软件展示用户个人金融信息，应满足《JR/T 0171-2020 个人金融信息保护技术规范》相关规定要求。

7.6.5 认证失败处理

客户端应用软件身份认证失败达到设定次数时，应提供临时冻结或永久冻结机制，保护客户账户安全。

7.6.6 密码的设定与重置

a) 提醒用户避免设置与常用软件、网站相同或相似的密码组合，并采取有效措施引导用户设置独立的密码。
b) 修改密码时对原密码输入错误次数进行限制，用户录入原始密码错误次数达到了限定次数时，应将用户账号锁定。
c) 密码设置可以引入人脸识别等辅助认证手段。

7.7 风险提示

a) 当移动金融客户端应用软件进入后台运行时，应提示客户应用软件已进入后台运行。
b) 移动金融客户端软件应具有防钓鱼风险提示能力，例如在客户登录时，显示客户预留信息方式，提示客户登录了正确的客户端。

c) 客户端应用软件应能防范客户密码泄漏风险，例如在客户长时间未修改登录密码时，应提示客户修改。
d) 客户端应用软件应具备交易重复提交风险提示，例如客户在一定的时间内提交相同转入方和金额的交易，客户端应用软件应提示客户重复提交风险。

7.8 缺陷解决率

针对客户端应用软件不同严重程度的缺陷，定义以下三种缺陷级别，并对其提出缺陷解决率要求：
a) 微小级别缺陷，即影响程度较轻的问题，如有个别错别字、文字排版不整齐等。该类缺陷对功能几乎没有影响，软件产品仍可正常使用。修复优先级最低，原则上要求尽快做出响应，并要求修复率达 95%。
b) 一般级别缺陷，即影响用户体验的问题，如次要功能模块丧失、提示信息不够准确、操作或响应时间长等。修复优先级中等，原则上要求当天内响应，并要求修复率为 99%。
c) 严重级别缺陷，即已经造成严重影响使用的问题。如系统崩溃、死机，或造成数据丢失、功能丧失；功能模块或特性没有实现，或致命的错误声明等。修复优先级较高，原则上要求立即作出响应，并要求修复率为 100%。

7.9 系统运维安全

a) 应对通信线路、主机、网络设备和应用的运行状况、网络流量等进行监测和报警，建立监测指标，有效监测、预警安全事件（风险），并及时采取应对措施。
b) 应对系统变更应做好风险评估、数据备份、应急预案、回退方案。对风险较大的变更，应做好变更后的监控及跟踪工作。

8 技术先进性

8.1 客户端兼容性要求

a) iOS 系统的移动终端适配机型要求：系统版本为 8.0 及以上，如 iPhone 6 及以上的 iPhone、iPad Air/Mini2 及以上的 iPad。
b) Android 系统的移动终端适配机型要求：系统版本为 5.0 及以上，建议适配 2016 年之后推出的主流旗舰机型。
c) 客户端 UI 应兼容不同分辨率和屏幕尺寸。
d) 客户端应用软件应保证客户端新旧版本在显示界面、功能、逻辑层面的兼容性。
e) 客户端应用软件应兼容 IPv6 协议。

8.2 客户端性能要求

a) 客户端的安装包大小应尽量精简，原则上要求安装包大小＜200M。
b) 客户端应用软件应具有快速的启动效率，原则上在主流机型上的冷启动时间≤1 秒。
c) 客户端应用软件应合理的使用内存资源，避免频繁的 GC 影响性能和大块申请，以及发生内存溢出问题；及时释放内存，以免发生内存泄漏。原则上在主流机型上内存占用率应≤10%。
d) 客户端应用软件应合理的使用 CPU 资源，避免占用过多 CPU 资源影响终端运行速度。原则上在主流机型上 CPU 占用率应≤30%。
e) 为保证客户端应用软件正常使用，后台服务器每秒联机交易并发数应不低于 100。
f) 客户端应用软件的后台服务器应具有良好的响应时间，要求其响应时间≤1 秒。

g) 客户端应用软件在进行 res 资源优化时，应避免短时间内大量图片的显示；UI 设计导出图片时应对图片进行无损压缩；此外还应对音频、文本文件等进行压缩。
h) 客户端应用软件在进行代码优化时，应尽量简化逻辑模块，移除无用的依赖库。
i) 客户端应用软件在进行 lib 资源优化时，除插件化的模块进行动态链接外，根据性能和应用程序的大小等因素综合考虑使用动态库方式还是静态库方式。

8.3 客户端更新要求

a) 客户端应用软件安装文件或补丁文件的打包、发布和维护等，应遵循严格审批流程。变更较大时，应进行安全检测和评估。
b) 客户端应用软件向公众发布前，可以采用白名单机制发布验证版本，进行小范围验证。
c) 应严格控制版本发布，避免发布未经充分测试、含有严重缺陷的版本。

8.4 与其它软件共存

a) 客户端应用软件测试过程中应注重共存性测试，保证不受与之共享资源的其他独立应用软件的安装、运行状况约束，能够良好共存；应不依赖于其它任何客户端程序独立运行。
b) 客户端应用软件应保证其安装资源的独立性和唯一性，避免同一终端安装不同版本的移动金融客户端软件。同时应避免应用软件被其他软件替换或删除。

9 创新及前瞻

9.1 服务创新

结合互联网产品设计趋势，探索新的交互及视觉设计方式，使产品设计能顺应移动端系统及用户操作习惯的变化。

9.2 技术前瞻性

9.2.1 大数据

a) 持续探索大数据应用技术在用户身份识别、行为识别、资信等级认定、网络环境识别等方面更深入应用。
b) 探索使用大数据对用户进行分析及建立用户画像，在客户个性化服务、安全校验、营销服务等方面发挥作用。

9.2.2 生物识别

持续探索使用人脸、指纹、声纹等多种生物特征领域应用：

a) 持续探索人脸识别技术深入应用，改进系统识别模型，提升正确识别率，技术相关指标逐步达到以下要求：人脸识别系统错误拒绝率降低到 5%以下，错误接受率降低到 0.001%以下。
b) 探索指纹识别在移动金融客户端上的应用，相关技术指标最终要求：错误拒绝率在 3%以下，错误接受率在 0.001%。
c) 探索声纹特征在移动金融客户端上的应用，相关技术指标最终要求：错误拒绝率在 3%以下，错误接受率在 0.5%。

9.2.3 人工智能

持续探索以下人工智能技术应用，推动业务发展：

a) 持续探索人工智能在智能客服领域的应用，可支持替代人工实现规范化和专业化的客户接待、业务办理、业务咨询、最新业务推介等服务。
b) 探索人工智能在业务风控上的应用，基于风险评估模型、机器学习等提升风险识别防控能力。