ICS 35.240.40
A 11

Q/GLB

桂林银行股份有限公司企业标准

Q/GLB 03—2023
代替 Q/GLB 03—2022

移动金融客户端应用软件安全管理规范

Financial mobile application software security management specification

企业标准信息公共服务平台
公开 2024年02月21日 09点14分

2020－8-31 发布　　2020－8-31 实施

桂林银行股份有限公司　　发布

目　　次

前　言

本文件根据GB/T 1.1-2020给出的规则起草。

本文件代替Q/GLB 03—2022《桂林银行移动金融客户端应用软件安全管理规范》，与Q/GLB 03—2022相比，除结构调整各编辑性改动外，主要技术变化如下：

a）增加了“生僻字的输入与显示”的要求内容（见8.1.3）；

本文件由桂林银行股份有限公司归口管理。

本文件起草单位：桂林银行股份有限公司。

本文件主要起草人：刘清萌、李玲华、黄积文、黎江维、韦玉谷。

本文件于2020年首次发布，2022年第一次修订，本次为第二次修订。

移动金融客户端应用软件安全管理规范

1 范围

本标准规定了桂林银行股份有限公司移动金融客户端应用安全要求，以及客户端应用软件设计、开发、维护和发布的管理要求。

本标准适用于本版本发布之日桂林银行股份有限公司提供的移动金融客户端应用。

2 规范性引用文件

下列文件对于本标准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标准。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 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0092-2019 移动金融客户端应用软件安全管理规范

3 术语与定义

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，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 capital transaction client application software

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

资讯查询类客户端应用软件 information query client application software

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。

3.4

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，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。

3.5

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。

3.6

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。

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）

URI：统一资源标识符（Uniform Resource Identifier）

TEE：可信执行环境（Trusted Execution Environment）

SDK：软件开发工具包（Software Development Kit）

SE：安全单元（Secure Element）

5 基本安全要求

5.1 身份认证

5.1.1 认证方式

认证方式应满足以下要求：

a）客户端应用软件登录时应采用适宜的验证要素，包括但不限于口令、短信验证码、手势密码、生物特征识别等方式。

b）应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，如：用于登录验证的口令和用于交易的口令不能一致。

c）客户端应用软件交易时应按照相关业务管理要求对用户身份进行认证，对于资金类交易，客户端应采用两种或两种以上要素对用户身份进行认证。对于单笔超过5万、当日累计超过5万的大额资金交易，客户端应用软件必须动态添加认证要素增强用户身份进行认证等级。

d）手势密码作为验证要素或验证要素组合中的一种时，要求手势密码应至少设置连续不间断的4个点。

e）短信验证码作为验证要素或验证要素组合中的一种时，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。

f）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。

g）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，应采取措施对用户身份重新认证。

h）客户端应用软件登录应采用两种或两种以上的要素对用户身份进行认证。

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：

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。

5.1.2.2 个人金融信息展示

个人金融信息应满足以下要求：

a）客户端应用软件的口令框应默认屏蔽显示，屏蔽时使用特殊字符（*）代替；

b）客户端应用软件禁止使用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，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、支付密码等）；

d）客户端应用软件展示个人金融信息时，处于已登录状态时，除银行卡有效期外，用户鉴别信息（如：卡片验证码、登录密码、支付密码等）不应明文展示，对于银行卡号、客户法定名称、手机号码、证件类或其他识别标识信息应脱敏展示。

5.1.2.3 认证失败处理

认证失败处理应满足以下要求：

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。

5.1.3 密码的设定与重置

密码的设定与重置应满足以下要求：

a）密码中至少包括字母、数字及其他键盘可输入的符号，密码的长度应不少于六位（银行卡密码、存折密码等长度一般为纯数字的客户密码除外），弱密码必须可被检测且禁止使用。

b）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。

c）使用初始登录密码与初始交易密码，必须强制用户修改初始密码。

d）在修改密码前，应对用户身份进行重新验证。

e）修改密码时应对原密码输入错误次数进行限制。

f）修改密码时新密码禁止与原密码相同。

g）在进行修改密码或密码重置时，除用户注册信息校核，还应采用两种或两种以上要素进行身份认证。

5.2 运维逻辑安全

5.2.1 运维逻辑安全设计

逻辑设计应满足以下要求：

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）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，必须遵循最小权限原则。

5.2.3 风险控制

a）应设计合理的登录风险控制策略。如：设置合理的账户登录超时控制策略；对于手机银行等APP应控制登录设备，当切换设备或者重新安装应用时应强制用户认证身份等；

b）应设计合理的交易风险控制策略。针对不同的资金交易金额，匹配不同的身份认证策略；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、时限控制策略等；

c）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）客户端应用软件禁止使用存在已知漏洞的系统组件与第三方组件；

b）客户端应用软件禁止使用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

a）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；

b）客户端应用软件应对传入的URI进行校验与安全处理，防止客户端应用软件运行异常或操作异常；

c）当客户端应用软件需要与TEE、SE结合使用时，应避免使用存在已知漏洞的接口。

5.3.3 抗攻击能力

a）客户端应用软件必须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）客户端代码必须使用代码加壳、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）客户端应用软件所使用安全输入控件必须具备抵御一定程度攻击的能力。

5.3.4 客户端应用软件环境检测

客户端应用软件在运行时应具备对运行环境的检查能力，并能向后台系统反馈设备信息等。

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；
c）应采用以国家标准或国家密码行业标准形式公开发布的密码算法（ZUC、SM2 、SM3、 SM4、SM9等）。

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禁止出现支付敏感信息，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禁止打印支付敏感信息；
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。

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，必须对关键交易数据进行安全签名，防止数据被篡改。

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

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，禁止访问非业务必需的文件和数据，禁止越权访问数据。

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）在客户端应用软件禁止与本地其他应用软件间传输时；

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，应采取措施数字签名确保其完整性；

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，应采取措施数字签名确保其完整性。

5.5.3.4 数据抗抵赖

客户端应用软件发起的资金类交易报文，采用数字证书进行签名，应确保交易报文的不可抵赖性。

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，必须防止重放攻击。

5.5.4 数据存储

5.5.4.1 个人金融信息存储

客户端应用软件禁止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。

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、身份证号码、手机号码、姓名等时应屏蔽关键字段。

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，文件系统中不允许残留任何个人金融信息。

5.5.6.2 页面返回保护

客户端应用软件应支持页面返回后自动清除银行卡密码、网络支付交易密码、登录口令等支付敏感信息的机制。

5.5.6.3 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 风险提示

移动金融客户端应在业务或交易有风险时，及时有效的进行风险提示，并应保障客户是否继续交易的选择权，不应替客户自动选择或执行，要求如下：

a）移动金融客户端软件进入后台时，应进行提示；

b）移动金融客户端软件运行时网络环境安全风险需要进行提示。提示信息的展示按本标准客户体验规范的信息展示要求。

5.7 缺陷管理

规范软件安全需求分析、安全设计、安全编码以及安全测试等工作，减少和控制软件安全漏洞和安全隐患，提高软件安全防护能力。客户端软件的缺陷应及时修复，要求如下：

a）缺陷分为严重缺陷、一般缺陷、轻微缺陷；

b）严重缺陷的缺陷修复率为100%，一天内修复；

c）一般缺陷的缺陷修复率为100%，一周内修复；

d）轻微缺陷修复率为98%，三周内修复。

6 管理要求

6.1 设计要求

客户端设计要求如下：

a）客户端应用软件系统架构安全设计上需考虑身份认证、WEB安全、行为抗抵赖、数据加密、防篡改、日志记录、安全漏洞监控等安全设计外，还需重点考虑服务器、终端和网络的安全设计；

b）根据系统安全级别要求，确定系统架构，尽可能采用集群或者双活模式，确实无法实现集群或者双活部署而且安全要求不高的可以采用主备模式；

c）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；

d）客户端应用软件后台应实现日志记录和分析功能，以对生产环境出现的问题进行监督、排查和审计；

e）客户端应用软件不得以默认、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；

g）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；

h）客户端应用软件应遵循合法、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；

i）客户端应用软件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；

j）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。

6.2 开发要求

客户端开发要求如下：

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；

c）客户端应用软件开发完成后，应同步完成产品手册、用户手册或提供在线帮助说明功能；

d）客户端应用软件的每次重要更新、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 发布要求

客户端发布要求如下：

a）客户端应用软件发布应由专门的应用管理人员负责，并在指定应用发布平台上进行发布管理；

b）客户端应用软件发布部署时，应根据实际情况，尽量使重要系统之间互相隔离、重要系统与其它系统之间隔离；

c）客户端应用软件应当删除调试或测试中存留的敏感数据；

d）客户端应用软件安装过程中，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；

e）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；

f）若客户端应用软件支持动态模块更新，应使用加密信道与服务端通信传输更新模块或对更新模块进行签名校验；动态模块更新后不得影响用户使用，不得修改用户已有的安全配置；

g）客户端须完成客户端软件实名备案，遵守《移动金融客户端应用软件安全管理规范》和中国互联网金融协会客户端备案的相关规范。

6.4 维护要求

客户端维护要求如下：

a）定期对客户端应用进行安全渗透性测试，保证新上线功能的安全；

b）对参与使用、管理、审计应用系统的用户进行权限分离，并采用最小权限原则防止过度授权；

c）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；

d）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；

e）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。

6.5 个人信息安全要求

6.5.1 收集

个人信息收集应符合GB/T 35273—2020和GB/T 41391—2022中6的要求，并应符合以下要求：

a）客户端应具有包含收集使用个人信息规则的隐私政策等收集使用规则；

b）客户端应在首次运行时通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

c）隐私政策等收集使用规则应便于用户访问，进入客户端主界面后访问隐私政策页面，应不多于4次点击等操作；

d）隐私政策等收集使用规则应便于阅读，包括但不限于提供简体中文版、文字大小合适、颜色明显、清晰等形式显示；

e）隐私政策等收集使用规则中应逐一列出客户端（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等信息；

f）收集使用个人信息的目的、方式、范围发生变化时，应以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等措施；

g）在客户端申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，应同步告知用户其目的，目的表述明确、便于理解；

h）有关收集使用规则的内容不应使用大量专业术语，应通俗易懂、简明扼要，便于用户理解；

i）个人金融信息收集应符合JR/T 0171—2020中6.1.1的要求。

6.5.2 传输

个人金融信息传输应符合JR/T 0171—2020中6.1.2的要求。

6.5.3 存储

个人信息存储应符合JR/T 0171—2020中6的要求，个人金融信息存储应符合JR/T 0171—2020中6.1.3的要求。

6.5.4 使用

个人信用使用应符合GB/T 35273—2020中7的要求，并应符合以下要求：

a）客户端应在征得用户同意后开始收集个人信息或打开可收集个人信息的权限；

b）客户端应在用户明确表示不同意后，不应收集个人信息和打开可收集个人信息的权限，不应频繁征求用户同意或干扰用户正常使用；

c）客户端实际收集的个人信用或打开的可收集个人信息权限不应超出用户授权范围；

d）客户端不应以默认选择同意隐私政策等非明示方式征求用户同意；

e）客户端应在用户同意后才可更改其设置的可收集个人信息权限状态；

f）客户端应允许用户关闭定向推送信息功能；

g）客户应以正当方式引导用户同意收集个人信息或打开可收集人个信息的权限，不应故意欺瞒、掩饰诱导用户；

h）客户端应向用户提供撤回同意收集个人信息的途径、方式；

i）客户端应遵守声明的收集使用规则收集使用个人信息；

j）客户端收集的个人信息类型或打开的可收集个人信息权限应与现有业务功能相关；

k）客户端用户不同意收集非必要个人信息或打开非必要权限，不应拒绝提供业务功能；

l）客户端新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，应提供原有业务功能（新增业务功能取代原有业务功能的除外）；

m）客户端收集个人信息的频度等不应超出业务功能实际需要；

n）客户端不应仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；

o）客户端不应通过要求用户一次性同意打开多个可收集个人信息的权限来限制客户对客户端的使用；

p）个人金融信息使用应符合JR/T 0171—2020中6.1.4的要求。

6.5.5 删除和销毁

个人信息删除和销毁应符合GB/T 35273—2020中8.3的要求，并应符合以下要求：

a）客户端应提供有效的更正、删除个人信息及注销用户账号功能；

b）客户端应为更正、删除个人信息或注销用户账号设置合理条件便于用于申请；

c）客户端应提供更正、删除个人信息及注销用户账号功能，并及时响应用户相应操作，需人工处理的，应承诺在时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理；

d）更正、删除个人信息或注销用户账号等用户操作应在客户端应和相应服务端后台共同完成；

e）客户端应建立并公布个人信息安全投诉、举报渠道，并在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）受理并处理；

f）个人金融信息删除和销毁应符合应符合JR/T 0171—2020中6.1.5和6.1.6的要求。

7 技术先进性要求

7.1 软件兼容性要求

客户端兼容性要求如下：

a）客户端支持的兼容终端数量应≥1000；

b）客户端安全运行操作系统版本支持安卓 7.0 以上、 iOS10以上；

c）移动金融客户端软件支持HarmonyOS(鸿蒙系统)；

d）网络兼容IPV4和IPV6。

7.2 性能要求

客户端应用服务器应要求如下：

a）安装包总体大小进行限制和优化限制：

1）移动金融客户端（安卓版本和 iOS版本）安装包应大小适中；

2）res文件中减少大图片的适配，减少重复的变量申请；

3）lib文件中应根据功能和业务需求减少非必要三方so文件的数量，删除无用的三方jar包；

4）dex 优化：不编译无用文件，对资源进行压缩处理，string(字符串）和color(色彩)资源优化，不超过65535个方法数（线性分配）；

5）代码优化：应采用删除无用代码、抽象重复代码、减少不必要的framework（程序框架)或者优化已有framework、Main(主函数>阶段优化、首次启动渲染页面优化等技术手段。

b）客户端软件的后台服务器高并发要求对重要的移动金融客户端，如手机银行，后台服务器应支持足够多的交易并发。重要客户端的后台服务器应支持400TPS以上的交易量；

c）客户端软件CPU占用率不应超过10%；

d）客户端软件内存平均占用率≤10%，内存峰值占用率≤50%。

7.3 反欺诈

客户端应用软件反欺诈措施要求如下：

a）应通过智能风险管理控制系统实时监测用户操作，发现违反常用操作进行提醒；

b）当用户发生敏感性、高风险性交易时，应进行风险提醒，并提供短信、密码校验、人脸识别等增强型用户身份认证手段，加强风险防控，降低欺诈风险；

c）应对客户端运行环境进行检测，当发现用户系统有root、越狱、修改rom、模拟器等风险时，应进行风险提示,并阻断登录、转账等交易；

d）预防仿冒软件措施：

1）应对全网渠道进行监测，通过深层次静态分析、动态分析、相似度分析等，精准对比正版应用与风险应用信息，第一时间发现潜在风险，保护客户合法权益，监测风险包括盗版、钓鱼仿冒、宣传仿冒等；

2）客户端应进行加固保护，预防通过反编译、静态分析、动态分析等逆向手段进行篡改后仿冒。

7.4 客户端更新

客户端更新应满足如下要求：

a）按照客户端升级方式，系统应提供客户端版本升级和静默热更新方式；

b）按照客户端升级范围，系统应提供全量版本升级和针对特定版本升级方式；

c）按照客户端升级类型，系统应提供客户端提示升级和强制升级方式。

8 创新及前瞻性要求

8.1 创新服务

8.1.1 无障碍使用要求

客户端无障碍使用要求如下：

a）无障碍设计应满足简洁性、易用性、稳定性和智能化要求：

1）简洁性：功能简洁、界面清晰、业务流程简明顺畅；

2）易用性：操作简单便利、信息易读易理解,设计大字体、大图标、文字高对比度等功能特点的大字版版本，页面字体应可跟随APP字体或系统字体调整，保证老年人或视力较差人群也可以清晰阅读和使用；

3）稳定性：具备容错性及兼容性，客户端用户视图切换应支持双向切换，切换过程宜无需重启APP；

4）智能化：智能语音、智能搜索。

b）无障碍设计应具有便利的引导流程，要求如下：

1）应制定功能变更使用指引说明，帮助客户掌握必要的操作技能；

2）系统在用户进行录入和选择操作时，及时校验用户输入信息准确性。系统在任务失败后，提示明确的出现错误信息并说明有效的解决方案；

3）在用户需要输入时，提供文本输入提示功能；

4）提供操作语音提示功能。

c）无障碍设计应采用创新性技术和应用措施：

1）支持读屏软件读屏；

2）支持标签按钮识读：对前端内部标签补全介绍，以便于读屏软件读取；

3）支持多媒体资源只读：将图片、利率展示等标签，补全成文本，保证视障人群可能清晰阅读；

4）支持一键反馈:提供快捷截图反馈功能，方便客户使用；

5）提供一键登录等便捷登录功能；

d）禁止广告插件：适老版界面、单独的适老版APP中严禁出现广告内容及插件，也不能随机出现广告或临时性的广告弹窗。禁止诱导类按键：移动应用程序中无诱导下载、诱导付款等诱导式按键。

8.1.2 人工智能金融服务

通过“数字人”实现“面对面”、“一对多”地人工智能金融服务。

基于人物形象建模技术、语音识别、语音合成、语义理解等人工智能技术，依托移动客户端打造虚拟“数字人”，提供填单辅助、交易查询、余额查询、资产负债、转账业务、客服答疑等金融服务。尤其为老年人等群体提供语音导航、语音辅助，优化服务体验流程，帮客户更高效地完成业务办理。

8.1.3 生僻字的输入与显示

通过开启“生僻字输入法”，可实现《金融服务 生僻字处理指南》（JR/T 0253-2022）“完整级”汉字的输入与显示。

用户进入手机银行“设置”页面，可选择开启“生僻字输入法”，启用该输入法后，可在转账业务、交易查询、资产负债等页面实现“生僻字”的输入与显示功能，帮助“生僻字客群”更准确、高效地完成业务办理。

8.1.4 扫码登录网上银行

通过客户端应用软件扫码的方式登录网上银行。

用户进入网上银行登录页，可选择二维码的方式进行登录。网上银行扫码登录能够降低用户使用网上银行的复杂度，降低用户输入的信息泄漏风险，用户使用网上银行更加方便和安全。

8.2 技术前瞻

8.2.1 指纹识别

移动金融客户端指纹识别应满足要求如下：

a）录入指纹信息发生变化时，移动金融客户端应自动注销客户指纹存储信息；

b）移动金融客户端识别出客户常用设备发生变化时，应自动注销客户指纹存储信息；

c）指纹特征注册、识别、变更、注销均由移动设备完成；

d）在指纹识别中，当设备认为通过时，成功率为100%。

8.2.2 人脸识别

移动金融客户端人脸识别应满足要求如下：

a）人脸识别不宜单独作为身份认证鉴别方法；

b）人脸识别应设置错误次数限制；

c）录入人脸面部信息发生变化时，移动金融客户端应自动注销客户面部存储信息；

d）移动金融客户端识别出客户常用设备发生变化时，应自动注销客户面部存储信息。

8.2.3 其它技术

客户端应根据业务需求和安全要求按需采用其它技术：

a）OCR识别技术：客户端通过拍照或上传生成银行卡、身份证照片、营业执照发送识别平台，平台进行算法处理生成最终识别出的证件信息的过程，通过OCR识别可大在提高业务操作效率以及简化繁琐的个人输入过程；

b）蓝牙技术：客户端可以通过蓝牙key等设备作为身份认证的一种方式登录或进行转账交易，蓝牙Key中存储了数字证书可以用来保证客户的信息安全，在移动设备端真正做到了“所见即所签”，交易安全便捷；

c）移动客户端开发平台：移动客户端开发平台具备消息推送、移动网管、发布服务、应用分析、数据同步等功能，卡顿情况<2%,流量异常<0.1%，数据同步推送>50条消息/S,冷启动<2S；

d）灰度测试：生产环境分为灰度版本（生产白名单版本）和正式生产版本，两套系统共用基础数据。灰度版本作为对正式生产版本的提前版本，验证APP更新、新增功能、上线流程的正确性，为正式对外提供验证保障，降低对外应用的缺陷率。灰度版本，应该遵循上线更新流程，制定上线方案、应急预案、验证方案。

参 考 文 献

[1] 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
[2] GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
[3] App 违法违规收集使用个人信息行为认定方法

企业标准信息公共服务平台
公开 2024年02月21日 09点14分