ICS 35.240.40
CCS A 11

Q/Bank of Qinhuangdao

秦皇岛银行股份有限公司企业标准

Q/Bank of Qinhuangdao 001—2023
代替 Q/Bank of Qinhuangdao 001—2022

移动金融客户端

Mobile Financial Client

2023－07－20 发布　　2023－08－01 实施

秦皇岛银行股份有限公司　发布

目　　次

前　言

本文件按照 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》的规定起草。

本文件代替Q/Bank of Qinhuangdao 001—2022《秦皇岛银行移动金融客户端》，与Q/Bank of Qinhuangdao 001—2022相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了“发布要求”的要求内容（见6.3，2022版的6.3）；

b) 增加了“无障碍服务体系建设案例”的内容（见9.1.2）。

本文件由秦皇岛银行股份有限公司提出并归口。

本文件起草单位：秦皇岛银行股份有限公司。

本文件主要起草人：项海南、吴頔、宣仰。

本文件及其所代替文件的历次版本发布情况为：

——2021年首次发布为Q/Bank of Qinhuangdao 001—2021，2022年第一次修订；

——本次为第二次修订。

移动金融客户端

1 范围

本文件规定了秦皇岛银行移动金融客户端应用软件的基本安全要求、管理要求、安全性要求、技术先进性要求和创新及前瞻性要求。

本文件适用于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。

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 38648-2020 信息安全技术 蓝牙安全指南

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

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 0098.3—2012 中国金融移动支付 检测规范 第3部分：客户端软件

JR/T 0171—2020 个人金融信息保护技术规范

3 术语和定义

GB/T 35273—2020、GB/T 39786—2021、JR/T 0092—2019、JR/T 0171—2020界定的术语和定义适用于本文件。

4 符号和缩略语

JR/T 0092—2019 界定的以及下列缩略语适用于本文件。

CDN：内容分发网络（Content Delivery Network）

CPU：中央处理器（Central Processing Unit）

GPU：图形处理器（Graphics Processing Unit）

HTTPS：安全超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）

IPv6：互联网协议第 6 版（Internet Protocol version 6）

OCR：光学字符识别（Optical Character Recognition）

SQL：结构化查询语言（Structured Query Language）

SSL：安全套接层协议（Secure Sockets Layer）

TLS：安全传输层协议（Transport Layer Security）

TPS：每秒事务处理量（Transaction Per Second）

5 基本安全要求

5.1 身份认证安全

5.1.1 认证方式

认证方式应符合JR/T 0092—2019中5.1.1的基本要求，并应符合以下要求：

a) 客户端首次登录应采用两种或两种以上的要素对用户身份进行认证；
b) 实名认证、重置登录密码、重置支付密码等重要交易时，应采用包含人脸识别及其他认证方式共两种或两种以上的要素对用户身份进行认证；
c) 在用户身份认证后，客户端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。

5.1.2 认证信息安全

5.1.2.1 安全输入

安全输入应符合JR/T 0092—2019中5.1.2.1的基本要求，并应符合以下要求：

客户输入的重要信息要具备即时防护功能，如：卡片验证码、卡片有效期、银行卡账号、身份证号码、手机号码等。

5.1.2.2 个人金融信息展示

个人金融信息展示应符合JR/T 0092—2019中5.1.2.2的基本要求和JR/T 0098.3—2012中7.3.3.3的通过标准。

5.1.3 认证失败处理

认证失败处理应符合以下要求：

a) 客户端应提供认证失败处理功能，设定连续认证鉴别失败次数阈值并在超出后锁定用户操作一段时间或采取结束会话、限制失败登录次数和自动退出等措施要求用户使用其他认证要素进行双重认证；
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

密码的设定与重置应符合以下要求：

a) 客户端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者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登录密码；
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） 在登录密码重置时，应使用短信验证码、用户注册信息校核等方式，对用户身份进行校验；
g） 在支付密码重置时，应采用两种或两种以上要素进行身份认证，如：数字证书、生物特征信息等；
h） 应采取有效措施提醒用户密码设置与常用软件、网站相同或相似的用户名和密码组合，并采取有效措施引导客户设置独立的支付密码。

5.2 逻辑安全

5.2.1 逻辑安全设计

逻辑安全设计应符合JR/T 0092—2019中5.2.1的要求，并应符合以下要求：
a）应在软件开发前对业务需求、集成方案等文档进行评审，避免出现逻辑安全漏洞；
b）应在软件测试阶段加入逻辑功能测试及渗透性测试，充分进行逻辑安全验证。

5.2.2 软件权限控制

软件权限控制应符合JR/T 0092—2019中5.2.2的要求，并应符合以下要求：
获取软件权限时，应先明确告知用户申请权限的用途。

5.2.3 风险控制

风险控制应符合JR/T 0092—2019中5.2.3的要求及JR/T 0098.3—2012中7.1.6的通过标准。

5.2.4 回退处理

回退处理应符合JR/T 0092—2019中5.2.4的要求。

5.2.5 异常处理

异常处理应符合JR/T 0092—2019中5.2.5的要求及JR/T 0098.3—2012中7.1.7的通过标准。

5.3 安全功能设计

5.3.1 组件安全

组件安全应符合JR/T 0092—2019中5.3.1的要求。

5.3.2 接口安全

接口安全应符合JR/T 0092—2019中5.3.2的要求。

5.3.3 抗攻击能力

抗攻击能力应符合JR/T 0092—2019中5.3.3的基本要求，并应符合以下要求：
客户端如使用安全输入控件，该控件应具备检测自身是否正在被调试的能力，并采取适当的风控措施，如：给予用户风险提示。

5.3.4 客户端应用软件环境检测

客户端应用软件环境检测应符合JR/T 0092—2019中5.3.4的要求及JR/T 0098.3—2012中7.2.1的通过标准，并应符合以下要求：
当客户端运行网络环境发生变化时，应提示用户。

5.3.5 SE 安全

SE安全应符合JR/T 0098.3—2012中5.3的通过标准，并应符合以下要求：

a) 用户可通过客户端查询 SE 中指定账户的信息；

b) 用户可通过客户端查询和修改 SE 中应用的交易参数。

5.4 密码算法及密钥管理

5.4.1 密码算法

密码算法应符合以下要求：

a) 客户端应使用商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

密钥管理应符合JR/T 0092—2019中5.4.2的要求，并应使用加密机存储密钥，客户端不存储密钥信息。

蓝牙相关密钥配置管理应符合GB/T 38648—2020中6.2的要求，并且使用的密码技术应符合国家密码管理相关规定。

5.5 数据安全

5.5.1 数据获取

5.5.1.1 数据防窃取

数据防窃取应符合JR/T 0092—2019中5.5.1.1的基本要求及JR/T 0098.3—2012中7.3.1.2的通过标准，并应符合以下要求：

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) 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。

5.5.1.2 数据防篡改

数据防篡改应符合 JR/T 0092—2019 中 5.5.1.2 的要求及 JR/T 0098.3—2012 中 7.3.1.3 的通过标准。

5.5.1.3 数据有效性

数据有效性应符合 JR/T 0092—2019 中 5.5.1.3 的要求。

5.5.2 数据访问控制

数据访问控制应符合 JR/T 0092—2019 中 5.5.2 的要求及 JR/T 0098.3—2012 中 7.3.2 的通过标准。

5.5.3 数据传输

5.5.3.1 通讯安全

通讯安全应符合以下要求：

a) 应在客户端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，应采用 TLS1.1 及以上版本的 HTTPS 协议进行通信；
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应用软件之间的安全认证。

5.5.3.2 数据保密性

数据保密性应符合JR/T 0092—2019中5.5.3.2的要求及JR/T 0098.3—2012中7.3.4.1和7.3.4.2的通过标准。

5.5.3.3 数据完整性

数据完整性应符合JR/T 0092—2019中5.5.3.3的要求及JR/T 0098.3—2012中7.3.4.3的通过标准。

5.5.3.4 数据抗抵赖

通过客户端发起的资金类交易报文，应采用数字证书技术确保交易报文的不可抵赖性。

5.5.3.5 数据防重放

数据防重放应符合JR/T 0092—2019中5.5.3.5的要求。

5.5.4 数据存储

5.5.4.1 个人金融信息存储

个人金融信息存储应符合JR/T 0092—2019中5.5.4.1的要求及JR/T 0098.3—2012中7.3.3的通过标准。

5.5.4.2 加密密钥存储

加密密钥存储应符合JR/T 0092—2019中5.5.4.2的要求。

5.5.5 数据展示

数据展示应符合JR/T 0092—2019中5.5.5的要求及JR/T 0098.3—2012中7.3.1.1的通过标准。

5.5.6 数据销毁

5.5.6.1 残余信息保护

残余信息保护应符合JR/T 0092—2019中5.5.6.1的基本要求，并应符合以下要求：

客户端应确保无法通过技术手段恢复已清除的敏感数据。

5.5.6.2 页面返回保护

页面返回保护应符合JR/T 0092—2019中5.5.6.2的基本要求，并应符合以下要求：

a) 客户端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) 当客户端从前台进入后台时，超过设定时限后应清除页面中已输入的敏感数据。

5.5.6.3 会话失效

会话失效应符合JR/T 0092—2019中5.5.6.3的要求。

5.6 风险监控

风险监控应符合JR/T 0068-2020中6.4.2.3中的基本要求，并且应符合以下要求：

应根据自身业务特点，建立完善的异常交易监控体系，可以采用设备指纹等技术进行识别并进行相应的控制，监测范围至少包括登录、查询、资金类交易以及与交易相关的行为特征、客户终端信息，来保证监控信息的安全性。

6 管理要求

6.1 设计要求

设计要求应符合JR/T 0092—2019中6.1的基本要求。

6.2 开发要求

开发要求应符合JR/T 0092—2019中6.2的要求及JR/T 0098.3—2012中4.1的通过标准，并应符合以下要求：

软件功能开发完成后，应根据需求文档对开发功能进行基础功能测试，渗透测试、安全性测试、性能测试、兼容性测试等。

6.3 发布要求

发布要求应符合JR/T 0092—2019中6.3的要求，并应按照金融行业主管部门有关规定，完成客户端软件实名备案等工作。

6.4 维护要求

维护要求应符合JR/T 0092—2019中6.4的要求。

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中5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GB/T 35273—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

个人信息使用应符合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息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） 客户端应以正当方式引导用户同意收集个人信息或打开可收集个人信息的权限，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） 客户端因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户申请；

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 JR/T 0171—2020 中 6.1.5 和 6.1.6 的要求。

7 安全性要求

7.1 身份认证信息

身份认证信息应符合以下要求：

a) 交易密码复杂度应符合以下要求：
   1) 不应设为重复的单一数字，如 111111 等；
   2) 不应设为连 6 位数字，如 123456 等；
   3) 不应设为证号、手机号等个人信息中连续 6 位；
   4) 不应设为与登录密码相同的密码。
b) 应采用无感身份认证、智能风控、设备认证、传统身份认证等方式中的两种或两种以上维度对用户身份进行认证：
   1) 无感身份认证：对用户行为进行分析，判断异常行为，如更换常用 IP 登录、多次登录失败、频繁登录等，APP 给出相应提示，并且，通过风控系统判断是否存在风险。
   2) 智能风控系统：利用反欺诈识别，智能风控利用多维度、多特征的数据预测用户的欺诈意愿和倾向；配置多套风控规则，组合使用，针对客户的不同行为作出预测判断，给用户提供不同响应方式，以起到防暴力破解、防撞库、防盗用、防核身异常的目的；
   3) 设备认证：客户初次使用 APP 或者更换设备使用 APP 时必须进行设备绑定，并且要提供多重用户信息进行验证。针对设备切换频繁的用户，风控系统也进行了监控与响应。

7.2 密码安全

7.2.1 密码应用方案制定

密码应用方案制定应以保障资金安全为核心，在保证安全的同时，具有足够的易用性，降低使用门槛。应综合采用以下技术进行安全防范：

a) 信息防篡改：采用数字签名技术，对关键信息进行签名；
b) 信息加密: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对传输信息进行加密处理；
c) 用户方（发起方）确认：针对一笔交易，通过动态口令、支付密码、FIDO+（快速安全身份认证系统）等技术确认用户身份；
d) 交易绑定：一笔交易使用一个无重复交易令牌，保障交易安全。

7.2.2 密码算法选择

密码算法选择应符合以下要求：

a) 客户端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机构要求的国产商用密码算法提出要求。
c) 密钥在传输过程中应使用密码算法对密钥进行保护。
d) 随机生成的密钥应具有一定的随机性与不可预测性。
e) 密钥应加密存储，并确保密钥储存位置和形式的安全。

7.2.3 密码策略应用

密码策略应符合以下要求：
a) 客户端应采用 TLS1.1 及以上版本的 HTTPS 协议与服务器后台通讯；
b) 客户端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对数据传输报文进行加密传输；
c) 服务器后台应采用加密机存储安全密钥，确保密钥储存位置和形式的安全。

7.2.4 密码安全性评估

密码安全性评估应符合以下要求：
a) 应符合密码应用安全性评估中的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置八项指标要求；
b) 应在信息系统规划阶段对密码应用方案进行评审或评估；
c) 应在信息系统建设完成后开展测评工作。

7.3 风险提示

应对客户端运行环境进行安全评测，并根据安全评测情况对客户进行风险提示：
a) 应对客户端运行环境的安全状况进行检测并向后台系统反馈，并将此作为风控策略的依据；
b) 应采取有效措施提升客户端环境安全级别，针对不同的安全等级采取相应的风险控制措施；
c) 应在门户站点等渠道发布客户端环境安全的提示；
d) 当发现客户端环境存在重大安全缺陷或安全威胁时，应采取必要措施对用户进行警示或拒绝交易；
e) 客户端如使用安全输入控件，该控件应具备监测自身是否正在被调试、截屏、录屏等情况的能力，并采取适当的风控措施，如：给予用户风险提示；
f) 当客户端切换到后台时应提示用户；
g) 应对客户端运行时的网络环境安全风险进行提示。

7.4 缺陷解决率

应每年对移动金融客户端及服务器进行渗透测试和安全评估，对于在渗透测试、安全评估等过程中发现的缺陷和漏洞应及时予以解决。

7.4.1 缺陷分类定级

缺陷分级定级应符合以下要求：
a) 一级：

1） 系统大面积或全面瘫痪，丧失重要服务能力；
2） 系统关键数据保密性、完整性、可用性遭到严重破坏；

b） 二级：
1） 信息系统的运行性能严重下降，整体服务能力受到极大影响；
2） 信息系统的运行出现短暂中断；

c） 三级：
1） 信息系统的运行性能明显下降，影响了服务效率；
2） 主要功能仍可正常提供服务；

d） 四级：
1） 信息系统的运行性能下降，小幅影响服务效率；
2） 主要功能仍可正常提供服务。

7.4.2 最低缺陷解决率

最低缺陷解决率应符合以下要求：

a） 一级风险的缺陷解决率=100%，2 小时内解决；
b） 二级风险的缺陷解决率=100%，4 小时内解决；
c） 三级风险的缺陷解决率≥80%，8 小时内解决；
d） 四级风险的缺陷解决率≥70%，8 小时内解决。

7.5 智能密码钥匙

智能密码钥匙包含目前普遍应用的USB Key、蓝牙Key、音频Key、SD Key等基于硬件的Key产品，也包括将来可能出现的其他基于硬件的Key产品。

智能密码钥匙应符合JR/T 0068-2020中6.2.2.1中的基本要求，并应符合以下要求：

a） 应能够自动识别其是否与客户端连接；
b） 应具备在规定的时间与客户端连接而未进行任何操作时的语音提示、屏幕显示提醒等功能。

8 技术先进性要求

8.1 兼容性

软件兼容性要求如下：

a） 客户端软件兼容终端型号数量≥1000；
b） 客户端软件安全运行支持的操作系统为安卓、iOS 和 HarmonyOS（鸿蒙系统）；
c） 客户端软件安全运行支持的操作系统最低版本为安卓 5.0、iOS 9；
d） 客户端软件兼容 IPv6 网络环境。

8.2 性能

客户端应用服务应符合以下要求：

a） 应对安装包总体大小进行限制并进行相应优化：
1） 客户端软件安装包文件大小不应超过 200MB；
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响应时间≤1 秒。
c) 客户端软件的后台服务器高并发要求如下：
1) 注册交易后台服务器支持并发用户数≥1%注册用户数，TPS≥300；
2) 单笔转账后台服务器支持并发用户数≥1%注册用户数，TPS≥1000；
3) 账户总览后台服务器支持并发用户数≥1%注册用户数，TPS≥500；
4) 存款产品支取后台服务器支持并发用户数≥1%注册用户数，TPS≥1000；
5) 我的账户查询后台服务器支持并发用户数≥1%注册用户数，TPS≥1000；
6) 存款产品购买后台服务器支持并发用户数≥1%注册用户数，TPS≥500。
d) 客户端软件 CPU 占用率要求如下：
1) CPU 平均占用率≤5%，CPU 峰值占用率≤60%；
2) 骁龙 660 AIE 八核处理器或同等以上性能设备，CPU 占用率≤40%；
3) 若为麒麟 955 八核处理器或同等以上性能设备，CPU 占用率≤10%；
4) 若为 A9 处理器或同等以上性能设备，CPU 占用率≤20%。
e) 客户端软件内存占用率要求如下：
1) 内存平均占用率≤10%，内存峰值占用率≤60%；
2) 若为高通骁龙 865 处理器 8GB 内存或同等以上性能设备，内存平均占用率≤20%；
3) 若为高通骁龙 865 处理器 12GB 内存或同等以上性能设备，内存占用率≤10%；
4) 若为 A7 处理器 1GB 内存或同等以上性能设备，内存占用率≤10%。

8.3 客户端更新

客户端需从服务端下载文件或补丁文件时，应保证下载通道的安全性，动态安装文件或补丁文件前应校验文件的完整性。

a) 更新之前，业务部门确定是否需要发布公告通知用户，若需通知用户，应在通知公告中明确更新内容、更新时间和更新方式；
b) 业务部门、技术部门应制定上线计划并执行。实施团队参与制定上线操作（应包含应用软件包部署、CDN 部署、SQL 语句、中间件部署等）方案，对上线过程中的各项内容应明确事件点、负责人、操作人和核验人；
c) 上线前技术部门、实施团队应分析上线可能出现的异常情况，并和业务部门共同制定回退方案；
d) 提前评估对下游数据影响，出影响评估报告，若有影响，提前 30 天通知下游系统修改。

8.4 软件共存

软件共存应符合以下要求：

a) 客户端软件在安装时应与其它正在运行的客户端软件之间允许共存；
b) 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。

8.5 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。

9 创新及前瞻性要求

9.1 服务创新

9.1.1 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。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；
   2) 易用性：操作简单便利、信息易读易理解（多感官通道、文本替代、语音读屏、统一交互），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，引导用户在功能发生变更后能及时熟悉、适应新功能，并指导用户使用新功能，帮助其掌握必要的技能；
   2) 系统在用户进行录入和选择操作时，及时校验用户录入和选择的信息，并提供相应提示，以提高用户输入的准确性。系统在任务失败后，为用户提示出现错误的原因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) 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) 多媒体资源识读：将图片、利率展示等标签，补全成文本，保证视障人群可以清晰阅读；
   4) 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；

6） 提供关键词记录功能；
7） 提供首页功能自定义功能；
8） 宜支持民族语言；
9） 宜提供自定义手势功能。

9.1.2 无障碍服务体系建设案例

为了给老年客户提供无障碍的移动金融服务，手机银行推出了“幸福生活版”功能，可一键切换至“幸福生活版”。

手机银行“幸福生活版”在设计上满足简洁性、易用性、稳定性和智能化要求，具备便利的引导流程，采用创新性技术和应用措施，支持智能搜索、语音转账、调整字号、定制首页等适老化及无障碍功能。

手机银行“幸福生活版”解决了老年客户在使用移动金融服务上遇到的困难，进一步完善了无障碍服务体系的建设。

9.1.3 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，点击左下角图标切换为二维码登录方式，使用已登录的客户端应用软件扫一扫功能扫描个人网银处展示的二维码进行登录，扫描二维码后，在客户端应用软件确认登录页点击确认登录后，个人网银可登录成功，若在确认登录页点击取消，则客户端应用软件返回扫一扫页面。

与传统登录方式相比，扫码登录更加便捷和安全。网上银行扫码登录能够降低用户使用网上银行的复杂度，提高用户线上办理业务的数量，降低银行线下服务成本。

9.1.4 语音转账

用户在客户端应用软件中通过语音交互的方式进行转账操作。

银行通过客户端应用软件向用户提供智能对话的交互形式来完成转账交易，为用户提供了一种新的转账方式，让用户在转账时多了一种选择。

与传统转账方式相比，语音转账功能可以让用户更加方便快捷的使用客户端应用软件进行转账交易，为老年人等群体提供更加贴切、更有温度的金融产品和服务，对提高品牌形象和增强用户粘性有很大帮助。

9.2 技术前瞻

9.2.1 生物识别技术要求

客户端应根据业务需求和安全要求按需采用生物识别等前沿技术，相关要求如下：

a） 生物特征识别系统指标要求：
   1） 指纹特征识别：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%；
   2） 人脸特征识别：人脸特征识别系统错误拒绝率≤5%的情况下，错误接受率应≤0.01%。
b） 生物特征识别系统技术创新与应用：
   1） 客户端采用快速安全身份认证系统 FIDO+作为登录、支付等重要业务的验证方式；
   2） FIDO+系统支持多种如“指纹认证”、“面部识别”等生物识别模式，提供安全、快捷、标准的身份验证方式。

3) FIDO+系统提供基于生物特征识别和 PKI 高强度密码认证的复合身份验证方式，采用 SM2、SM3、SM4 等国产密码算法，使用多级密钥体系，协议安全经过了形式化证明。

c) 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 识别可大大提高业务操作效率以及简化繁琐的个人输入过程。

d) 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，在进行登录、转账交易时，根据用户已开通的验证方式显示可切换的安全认证组合方式，在用户使用、动账交易更安全便捷。在人脸识别时，记录场景信息。

e) mPaaS 开发平台：mPaaS 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，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。

f) 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。

9.2.2 设备指纹

客户端应用软件通过集成设备指纹系统，在登录时判断应用环境的潜在风险和漏洞，再通过风险标签判断是否予以登录。

该业务功能是在登录时检测运行环境，返回风险标签，对于伪造ztoken、模拟器、云手机、视频流劫持、设备篡改等高风险标签予以拒绝登录；对于IMEI格式不合法、VPN/代理、非厂商ROM、改码工具、按键精灵等低风险标签需要进行短信二次核身通过后方可继续登录流程;对于无风险标签可直接继续登录流程。

该业务功能有效的增强了业务风险控制能力，提高了设备的安全性。

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