ICS 03.060
CCS A 11

Q/CMBC

中 国 民 生 银 行 企 业 标 准

Q/CMBC 004—2023
代替 Q/CMBC 004—2022

中国民生银行手机银行移动金融客户端应用标准

Enterprise standard of financial mobile application of China Minsheng Bank

2023 - 11 - 15 发布　　2023- 11 - 15 实施

中国民生银行　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/CMBC 004－2022《中国民生银行手机银行移动金融客户端应用标准》，与Q/CMBC 004－2022相比，除了编辑性改动外，主要的变化为：在第6.1条中增加无障碍服务体系建设案例。

本文件起草单位：中国民生银行股份有限公司。

本文件主要起草人：刘衍波、陶江、蔡丹平、崔宇程、石菁菁、吴欣、李晓东、楼晔、虞刚、谢军、宋宏、臧涵博、温彦杰、袁丽欧、袁靖、王广驰、聂建军、李晓、龚正、林潇、樊凯、郝斌斌。

本文件及所替代文件的历次版本发布情况为：

——2020 年首次发布 Q/CMBC 004—2020；

——2021 年第一次修订 Q/CMBC 004－2021，代替 Q/CMBC 004—2020；

——2022 年第二次修订 Q/CMBC 004－2022，代替 Q/CMBC 004—2021；

——本次为第三次修订。

引　言

近年来，伴随移动通讯的快速发展，移动金融客户端已经成为银行业面向客户的重要服务渠道。然而，由于移动通讯特有的风险特性导致移动金融客户端存在一些诸如信息泄露、资金损失、交易纠纷难以有效解决等问题和风险。在这样的情况下，提升移动金融客户端的服务质量对整体提升我国银行业的服务水平意义重大。

为提升中国民生银行手机银行移动金融客户端服务水平，增加移动金融客户端应用领域的标准供给，促进金融风险防控、消费者权益保护，中国民生银行发布《中国民生银行手机银行移动金融客户端应用标准》，对发挥企业标准引领质量提升、促进消费升级和推动移动金融业务转型升级等方面具有重要意义。

本文件参照国家、金融行业相关标准，根据业界当前的实践，采用半形式化的方法给出了移动金融客户端的主要服务功能及属性，主要涉及安全性、技术先进性、创新及前瞻性、实施保障四个方面，旨在明确中国民生银行手机银行移动金融客户端应用企业标准，促进手机银行移动金融客户端应用规范、健康发展。

中国民生银行手机银行移动金融客户端应用标准

1 范围

本文件规定了本行手机银行移动金融客户端应用要求，明确了手机银行移动金融客户端应用安全性、技术先进性、创新及前瞻性标准，确立了手机银行移动金融客户端应用实施保障机制。

本文件适用于本行手机银行移动金融客户端。

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。

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

GB/T 19000—2016 质量管理体系 基础和术语

GB/T 27912—2011 金融服务 生物特征识别 安全框架

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

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

GM/T 0029—2014 签名验签服务器技术规范

GM/T 0030—2014 服务器密码机技术规范

JR/T 0068—2020 网上银行系统信息安全通用规范

JR/T 0071.2—2020 金融行业网络安全等级保护实施指引 第2部分：基本要求

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 0118—2015 金融电子认证规范

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0231—2021 银行业第三方软件开发工具包（SDK）安全接入指南

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。

[来源：JR/T 0092—2019，定义2.1]

3.2 客户端 APP (application)

基于软件的提供部分或全部服务的机制。

3.3 **移动应用** mobile application

在移动设备上运行的应用软件。

[来源：GB/T 37668—2019，定义2.2]

3.4 **服务** service

至少有一项活动必需在组织和客户之间进行的组织的输出。

3.5 **客户** customer

已经或将要发生直接交易关系的对象。

注：在本文件中，顾客与客户视作同义词，并均可简称为客户。

3.6 **产品** product

在组织和顾客之间未发生任何交易的情况下, 组织能够产生的输出。

[来源：GB/T 19000—2016，定义3.7.6]

注：在本文件中，仅考虑通过手机银行移动金融客户端的服务向顾客提供产品和支撑产品运作的情况。

4 服务安全性

4.1 基本安全要求

4.1.1 安全技术标准

4.1.1.1 安全技术通则

手机银行移动金融客户端安全应符合JR/T 0092—2019、JR/T 0171—2020、GB/T 35273—2020、GB/T 27912—2011、GB/T 39786—2021、GM/T 0030—2014、GM/T 0029—2014、JR/T 0068—2020、JR/T 0071.2—2020、JR/T 0098.3—2012、JR/T 0118—2015、JR/T 0231-2021等相关标准的要求。

4.1.1.2 移动金融客户端软件

4.1.1.2.1 逻辑安全设计

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) 移动金融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。

4.1.1.2.2 软件权限控制

a） 移动金融客户端程序应禁止访问终端中非业务必需的文件和数据；

b） 应根据最小权限原则申请系统权限（例如，申请读取通讯录、地理位置等权限），应遵循最小权限原则，并取得用户的明示同意。

4.1.1.2.3 风险控制

a）应设计合理的登录风险控制策略，包括但不限于：

1） 当用户闲置在线状态超出时限时，应设计合理的账户登录超时控制策略；

2） 合理的多点登录策略，如：提示登录信息或退出先登录的账户等策略；

3） 合理的长期未登录控制策略，当用户长时间未登录时，应综合考虑风险情况，增大认证强度。

b） 应设计合理的交易风险控制策略，包括但不限于：

1） 针对不同的资金交易金额，应设计合理的身份认证策略；

2） 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） 移动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。

4.1.1.3 安全功能设计

4.1.1.3.1 组件安全

a） 移动金融客户端应用软件应避免使用存在已知漏洞的系统组件与第三方组件；

b） 移动金融客户端应用软件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；

c） 移动金融客户端程序开发设计过程中应注意规避各系统组件、第三方软件开发工具包（SDK）存在的安全风险，应对开发框架和技术路线进行严格的论证，必要时应进行选型安全测试。涉及密码运算的组件应具备国家商用密码管理部门颁发的认证证书，并定期进行第三方安全检测。

4.1.1.3.2 接口安全

a） 移动金融客户端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） 移动金融客户端软件应对传入的 URI 进行校验与安全处理，防止客户端软件运行异常或操作异常；

c） 当移动金融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。

4.1.1.3.3 环境检测

客户端应用软件在运行时具备对运行环境的检查能力，检查的范围应包括：系统是否越狱或 root、程序运行环境是否可信（例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环境信息等。

4.1.1.3.4 抗攻击能力

a） 移动金融客户端应具备抗攻击能力，包括但不限于抵御静态分析、动态调试、保持自身完整性、真实性，防止篡改及注入的功能；

b） 移动金融客户端代码应使用代码加壳、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） 移动金融客户端应用软件应进行签名，签名证书能有效标识应用软件的来源和发布者，保证客户所下载的客户端程序来源于所信任的机构；

d） 移动金融客户端具有已知漏洞的防范能力。

4.1.1.4 移动金融客户端通讯安全

通讯安全指移动金融客户端与服务器端间网络安全，包括以下内容：

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） 采取的安全协议应包括但不限于 SSL/TLS 或 IPSec，应采用 SSL3.0/TLS1.0 以上；

d） 移动金融客户端应用软件应支持通过 IPv6 连接访问网络服务，在 IPv4/IPv6 双栈支持的情况下，优先采用 IPv6 连接访问，移动应用图标或启动界面应显性显示 IPv6 标识；

e） 移动金融客户端应用软件在 IPv6 环境下，分时段发起移动应用连接的失败率不应超过 5%；
f） 移动金融客户端应用软件分别在 IPv6 和 IPv4 环境下连接时间不应有明显差异，分时段发起应用连接，访问延迟均值应小于 15%或 75ms（二者中取最大值）；
g） 移动金融客户端应用软件与服务器应至少进行单向认证，可通过密钥、证书等密码技术手段实现安全认证，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。在 SSL 加密链接的基础上，移动金融客户端应用应增加对交易报文的加密，防止敏感信息泄露及篡改；
h） 敏感数据在本地程序组件间或通过公共网络传输时，应采取措施（如加密等）确保其保密性；若本地其他应用软件不能提供与本移动应用相应等级的加密接口，则应评估敏感数据调用的风险，并设计补救措施；
i） 关键交易数据在本地程序组件间或通过公共网络传输时，应采取措施（如数字签名、MAC 等）确保其完整性；
j） 应用软件发起的身份认证类或资金类交易报文应能够防止重放攻击。

4.1.1.5 移动金融服务器端安全

服务器端安全指服务器端应用程序安全，包括以下内容：
a） 应用系统应具有防请求重放机制；
b） 对于文件上传和文件下载，应注意控制文件类型，限制文件目录的权限，防止前端越权访问；
c） 服务端在验证短信验证码时，应使用客户预留的可信手机号码进行校验，防止越权使用；
d） 对于短信验证码认证与交易操作分步执行的情况，应在认证通过后分配认证标识，与用户信息绑定，且使用一次后失效。

4.1.1.6 数据安全

基本要求：
a） 应遵照有关法律法规和行业制度规定，严格遵照客户意愿和指令进行支付，不得泄露用户支付敏感信息；
b） 与外部机构应对发送的报文计算摘要或进行签名，保证数据报文的完整性，计算摘要或进行签名运算的数据应包含报文中的关键信息；
c） 与外部机构均应对发往对方的报文进行传输加密，加密信息应包括报文中的关键信息和客户敏感信息；
d） 与外部机构应拥有具有电子认证服务许可证的证书颁发机构颁发的数字证书，并使用符合国家密码主管部门要求的签名算法，对报文摘要数据进行规范化处理后，进行数字签名，保证交易行为的不可抵赖性；
e） 应依据《中国人民银行关于进一步加强银行卡风险管理的通知》等文件要求，对支付敏感信息的采集、展示、传输、存储、使用等环节制定保护策略，并定期开展支付敏感信息安全的内部审计。

4.1.1.7 个人信息安全

应对客户的身份信息、认证信息、账户信息、交易信息等个人信息进行严格保护，制定相应的相关管理制度，在管理制度中对客户个人信息等进行明确分类分级定义。

个人金融信息保护措施应覆盖个人金融信息收集、存储、传输、使用、删除、销毁等完整全生命周期环节，具体包括：

a） 个人金融信息的收集，应符合以下原则：

1) 移动金融客户端收集个人金融信息前，应通过隐私政策等方式向个人金融信息主体明确告知金融产品（包含集成的第三方组件）需收集的个人金融信息的类别、目的、方式和范围，以及收集、使用个人金融信息的规则，并获得个人金融信息主体的明示同意；
2) 在移动金融客户端上输入个人信息时，就使用加密等技术保证数据的保密性，防止用户输入的数据被其他程序非法获取；
3) 移动金融客户端不得以欺诈、诱骗，或默认授权、功能捆绑等方式误导、强迫个人金融信息主体提供个人金融信息，不得违反与用户的约定收集使用个人金融信息；
4) 移动金融客户端不得故意隐瞒产品或服务所具有的收集个人金融信息的功能；
5) 移动金融客户端不得收集法律法规与行业主管部门有关规定明令禁止收集的个人金融信息；
6) 移动金融客户端收集个人金融信息应遵循最小化要求，仅收集与实现和优化金融产品或服务、防范金融产品或服务的风险所必须的信息；
7) 移动金融客户端收集年满 14 周岁未成年人的个人金融信息前，应征得未成年人或其监护人的明示同意，不满 14 周岁的，应征得其监护人的明示同意；
8) 移动金融客户端首次启动时，应采取技术措施（如弹窗、明显位置 URL 链接等），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，方可开展有关个人金融信息的收集活动；
9) 移动金融客户端自动采集个人金融信息的频率应是实现产品或服务的业务功能所必需的最低频率；
10) 用户在进入移动应用主页面后，应至多经过 4 次点击便可访问到隐私政策或个人金融信息的收集使用规则；
11) 移动金融客户端应制定隐私政策，具有简体中文版，易于阅读，不应给用户造成阅读或理解障碍，且内容符合《信息安全技术 个人信息安全规范》（GB/T 35273-2020）中的相关要求，隐私政策中应包含隐私政策变更的原因以及用户访问更新后隐私政策的途径；
12) 若移动金融客户端具有利用用户个人金融信息和算法向个人推送信息的功能，则应向用户提供关闭该服务的功能，且在用户关闭后不得自动开启或延期自动开启；
13) 在停止提供金融产品或服务时，应及时停止继续收集个人金融信息的活动。

b) 个人金融信息的存储，应符合以下原则：
1) 客户端不应留存非本机构的银行卡磁道数据、银行卡有效期、卡片验证码(CYN 和 CYN2)、银行卡密码等 C3 类别信息，敏感个人金融信息及其密文在使用后应立即清除；客户端存储一般个人金融信息时，应采取相匹配的安全措施进行防护处理；
2) 服务器存储个人金融信息，应根据个人金融信息自动和非自动处理的特点，制定相应的数据安全保护策略，包括访问控制、权限设置、密钥管理等，防止个人信息的不当使用、毁损、泄露、删除等；
3） 应采取必要的技术和管控措施保证个人金融信息存储转移过程的安全性；
4） 个人金融信息的存储应依据个人信息主体授权使用的目的所必需的时间，严格依据隐私政策的规定要求，法律法规另有规定或个人信息主体另行授权同意的除外；
5） 超出上述个人金融信息存储期限后，应对信息进行删除或匿名化处理；
6） 应定期备份存储的个人金融信息，保证备份、恢复的完整性、可靠性和准确性。

c) 个人金融信息的使用，应符合以下原则：
1) 敏感个人金融信息中的个人认证信息不能以任何形式下发到客户端；认证信息的比对只能在服务器进行；敏感个人信息中的个人身份信息在下发至客户端之前，应屏蔽个人身份信息中不可猜测的一部分，被屏蔽部分使用统一的符号替代；

2) 对于银行卡号、手机号、证件号等 C3 类个人金融信息应进行屏蔽展示或去标识化处理，或由用户选择是否屏蔽展示，如需要完整展示，应进行用户身份验证，并做好数据的管理，数据泄露风险；
3) 对被授权访问个人金融信息的人员，应建立最小授权的访问控制策略，进行分级授权访问，遵循“最小必要”的原则对数据进行使用；
4) 采用专门用于测试的测试账户进行开发测试，真实个人信息不得用于开发测试；
5) 应采取必要的技术手段和管理措施，确保个人金融信息清洗或转换过程中对信息进行保证，对 C2、C3 类别信息，应采取更加严格的保护措施；
6) 应对个人金融信息的访问行为进行监测，对其操作过程 进行日志记录，记录内容包括但不限于日期、时间、主体、事件措施、事件结果等。

d) 个人金融信息的传输，应符合如下原则：
1) 应采用满足个人金融信息传输安全安全控制措施，对传输个人信息的通信过程中的整个报文或会话过程进行加密；
2) 传输个人金融信息前，通信双方应通过有效技术手段进行身份鉴别和谁；
3) 个人金融信息传输的接收方应对接收的信息进行完整性校验；
4) 应建立有效机制对个人金融信息传输进行监测，并对传输安全策略进行审核和优化；
5) 应采取有效措施保证数据传输可靠性和网络传输服务可用性。

e) 个人金融信息的删除，应符合如下原则：
1) 应采取技术，在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问；
2) 个人金融信息主体要求删除个人金融信息时，应依据国家法律法规、行业主管部门有关规定以及个人金融信息主体的约定予以响应。

f) 个人金融信息的销毁，应符合如下原则：
1) 应制定严格的个人信息销毁制度，确保应记录个人信息的相关的文档、介质得到及时、有效的销毁，个人信息销毁前应得到相应的授权；
2) 对于以下保存到期或已经使用完毕的个人信息，均应建立严格的销毁登记制度：纸质、光盘、磁带及其它可移动的数据存储载体等介质中存储的个人信息；报废设备或介质中存储的个人信息； 其他超过保存期限需销毁的个人信息；
3) 应保证存储敏感个人信息的介质在销毁后，信息不可恢复；
4) 对于所有需销毁的个人信息，应在双人控制、监督人员在场情况下，采取有效措施，及时妥善销毁。

4.1.1.8 安全管理

应设立专门的安全管理机构，对手机银行移动金融客户端的安全制定相关制度办法，包括以下内容：

a) 应明确安全管理机构和其他各相关机构的职责范围、工作流程和沟通协调机制；
b) 宜按照系统应用架构、系统使用人员、访问终端类型、发布方式等方面进行安全评估，确定移动金融 AP 的安全风险等级；
c) 应为手机银行移动金融客户端建立安全评估机制，对新系统上线和系统变更制定全生命周期的安全评估机制，具备安全事件的应急处理能力；
d) 应为手机银行移动金融客户端建立源代码安全检查机制，对缺陷整改情况进行跟踪；
e) 宜为手机银行移动金融客户端建立定期安全渗透测试和漏洞检查机制，对漏洞库进行统一管理，并持续跟踪漏洞修复状况；

f） 应为手机银行移动金融客户端建立安全风险分析及处理机制，针对用户异常行为和系统攻击可以进行追踪溯源。

4.2 身份认证

基本要求：

a） 移动金融客户端应用软件登录时应采用适宜的验证要素，包括但不限于密码、短信验证码、手势密码、 生物特征识别、FIDO 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：用于登录验证的密码和用于交易的密码不能一致；

c） 移动金融客户端应用软件进行资金类交易或重要客户信息修改交易时应使用双因素认证。双因素身份认证由以下三种身份认证方式中至少两种组成：一是客户知悉的要素，如静态密码等；二是客户持有的，不可复制或者不可重复利用的要素，包括但不限于物理介质、电子设备等；三是客户的生物特征要素，如指纹、虹膜、声纹等；

d） 对于手势密码、短信验证码、生物特征信息作为验证要素或验证要素组合中的一种时，应满足如下要求：

1） 密码策略：若采用密码作为验证要素，应采取措施对密码复杂度进行校验，保证密码达到一定的强度，宜避免采用与客户生日、手机号等个人信息相似度过高的密码；

2） 若采用手势密码作为验证要素，手势密码应至少设置连续不间断的 4 个点，至少两个折点；手势密码可在系统登录、应用从后台返回等场景中使用，不能在以下场景中作为验证用户身份的凭据，包括交易验证、修改登录密码、开户等；手势密码不应保存在客户端，应以加密形式保存在服务器端；设备更换时应强制重新设置手势密码；

3） 若采用短信验证码作为验证要素，短信验证码应仅使用一次，仅限于在规定时间（1 分钟）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；使用的短信验证码应与交易要素进行绑定，并采用支持国产密码算法的硬件加密设备生成；

4） 若采用生物特征识别作为验证要素，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，并且相关技术要满足如下指标：

—对于指纹特征识别技术，错误接受率≤0.001%情况下，错误拒绝率≤3%；

－对于人脸特征识别技术，错误接受率≤0.01%情况下，错误拒绝率≤5%。

e） 图形验证码不得作为独立的身份验证要素，在使用图形验证码作为验证的辅助要素时，图形验证码应具有使用时间限制并仅能使用一次，图形验证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容；

f） 应有独立的支付密码，并保证支付密码和登录密码不同；

g） 连续认证失败次数超过阀值后应进行锁定，移动金融客户端退至后台闲置时间超过阀值时应重新认证；

h） 移动金融客户端应用软件在输入账户登录密码、银行卡支付密码和网络支付交易密码等认证信息时，不可明文显示，应采取替换输入框原文、逐字符加密、字符加密、防范键盘窃听、使用安全键盘，以及其他手段，确保用户输入的认证信息明文的安全；

i） 移动应用应为客户输入的卡片验证码、卡片有效期、银行卡账号、身份证号、手机号等信息提供安全防护；

j） 移动金融客户端应用软件的口令框应默认脱敏或屏蔽显示，且脱敏或屏蔽显示时使用同一特殊字符代替；

k） 移动金融客户端应用软件处于未登录状态时，不应展示与个人金融信息主体相关的用户鉴别类别信息；

l） 除银行卡有效期外，用户鉴别信息（包括但不限于银行卡密码、网络支付密码、卡片验证码（CVN 和 CVN2）、账户登录密码、账户查询密码、交易密码等）不应明文展示；

m） 对于银行卡号、手机号码、证件类识别标识或其他识别标识信息的关键信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证；涉及其他信息主体的信息时，移动应用对显示的信息应进行屏蔽展示。

增强要求：

a） 移动金融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；

b） 在用户身份认证后，移动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；

c） 宜结合移动金融客户端环境安全级别，针对不同的安全等级采取相应的身份认证策略，在安全的同时提升客户体验。

4.3 密码安全

4.3.1 密码应用方案

基本要求：

a） 结合《JR/T 0197-2020 金融数据安全数据安全分级分类指南》排查三、四级数据的存储情况，四级数据输入、传输和本地存储环节不应出现明文或非商用密码加密情况；

b） 移动金融客户端所使用的身份鉴别、数据传输安全、客户端数据存储、交易抗抵赖等密码应用安全组件均应支持且优先使用商用密码算法；

c） 应采用商用密码算法对登录用户进行身份鉴别（包括但不限于银行卡密码、网络支付密码、卡片验证码（CVN 和 CVN2）、账户登录密码、账户查询密码、交易密码等），保证用户身份的真实性；

d） 应采用商用密码算法对交易报文及关键业务要素进行保护，保证交易数据在传输过程中的机密性；

e） 应采用数字签名对资金类交易及重要客户信息修改交易进行抗抵赖保护，保证交易在传输过程中的完整性；

f） 应采用商用密码算法对移动金融客户端的完整性进行保护，并对其发布者进行身份鉴别；

g） 应采用商用密码算法对客户端存储的数据进行保护，保证数据在存储过程中的机密性和完整性。

4.3.2 密码算法

基本要求：

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符合国家密码主管部门的要求。密钥长度应满足下列要求：

1） 对称密码算法：SM4、AES、3DES 算法的密钥长度满足 128 位及以上；

2） 非对称密码算法：SM2，使用 256 位及以上的密钥长度；RSA，使用 2048 位及以上的密钥长度；

3） 散列算法：SM3、SHA256 及以上。

4.3.3 密钥管理

基本要求：

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；

d） 用于移动金融客户端的身份鉴别、数据传输、客户端数据存储等场景信息加密的密钥应随机生成，且随机数应在服务端产生。

4.3.4 密码安全性评估

基本要求：

a） 建立移动金融客户端中所使用的密码算法第三方软件开发工具包（SDK）信誉库，制定安全准入和安全性评估机制；

b） 建立商用密码算法应用安全性评估机制，针对移动金融客户端的身份鉴别、数据传输安全、客户端数据存储、交易抗抵赖等场景进行算法实现方案评估。

4.4 实名备案

基本要求：

a） 移动金融客户端首次在官方渠道、应用市场发布或者备案后发生重大变更需要更新发布的,金融机构至少在官方渠道或应用市场发布前 40 个工作日向中国互联网金融协会申请实名备案；

b） 移动金融客户端备案后发生一般变更的,金融机构应在官方渠道或应用市场更新发布前 10 个工作日向中国互联网金融协会提交办理备案变更申请；

c） 对于服务停止或下架的移动金融客户端, 金融机构应在服务停止或下架实施前向中国互联网金融协会提交办理注销备案申请。

4.5 风险提示要求

手机银行移动金融客户端应对交易事前、事中及事后的风险防控提出规范和要求，包括以下内容：

a） 移动金融客户端应用软件如使用安全输入控件，应具备检测自身是否正在被调试的能力及终端环境威胁感知能力，当感知到风险时，采取适当的风控措施，如：给予用户风险提示、增强认证、延缓交易等；

b） 应对交易过程进行账户级风险识别与干预，对于包括用户注册、登录、支付、转账、绑卡、贷款等风险进行识别，防范潜在的非法交易、欺诈交易；

c） 应建立交易监控的相关系统，能够甄别并预警潜在风险的交易；应建立反洗钱监测平台，并建立可疑交易监测标准，识别包括套现在内的主要洗钱犯罪；应建立业务安全威胁分析预警平台，收集行内客户行为数据以及外部情报，进行客户行为分析，构建客户画像，识别业务安全威胁；宜建立欺诈交易侦测平台，在交易过程中结合欺诈交易风险特征，采取电话、短信等方式进行风险识别与审查；

d） 应根据交易的风险特征建立风险交易模型，有效监测可疑交易，形成客户信息与账户管理、客户账户交易、授信及资产业务等业务类型的风险交易模型，对可疑交易建立报告、复核、查结机制；

e） 应对监控到的风险交易进行及时分析与处置。并建立风险事件库，用于模型优化和管理提升；

f） 客户端切入后台如果需要继续处理某些功能时，要予以客户明确提示；

g） 客户端进入新的 wifi 网络环境要予以风险提示要求。

4.6 缺陷解决率

4.6.1 缺陷分类

a）致命缺陷：部分用户APP无法启动，部分用户核心功能无法正常使用；
b）严重缺陷：用户某个业务功能无法使用；
c）一般缺陷：一定比例的用户在使用特定业务功能时，出现一些不影响正常使用的显示性错误；
d）偶现缺陷：某些特定条件下，某个特定功能偶发一些显示性错误。

4.6.2 缺陷修复率要求

a）待发布版本致命缺陷和严重缺陷遗留个数应为0；
b）一般缺陷遗留个数不应超过3个；
c）偶现缺陷遗留率应≤10%。

5 技术先进性

5.1 兼容性要求

5.1.1 兼容终端数量

兼容主流移动设备终端，主流的Android终端设备和iOS终端设备数量≥1000（终端数量=测试机型×系统版本）。

5.1.2 操作系统兼容性

a）应兼容iOS9.0版本及其以上操作系统；
b）应兼容Andriod5.0版本及其以上操作系统；
c）应兼容HarmonyOS系统。

5.1.3 网络环境兼容性

应支持国内三大运营商移动网络，支持WIFI网络，并兼容IPv6网络环境。

5.2 性能要求

5.2.1 安装包大小

a）客户端应尽量精简安装包大小，去除冗余资源，方便客户下载使用；
b）iOS安装包大小不宜超过300M；
c）Android安装包大小不宜超过150M。

5.2.2 服务响应时间

客户端内页面加载显示时间，平均≤0.5秒，页面加载完成时间平均≤1秒。

5.2.3 服务器并发量

客户端后台服务器应具备每100万日活用户至少10万级QPS请求的能力。

5.2.4 CPU 占用率

客户端应该尽量控制CPU占有率，并持续作监测和优化。主流移动设备总的内存占有率尽量不超过系统10%。

5.2.5 内存占用率

客户端应该尽量控制内存占有率，并持续作监测和优化。主流移动设备总的内存占有率尽量不超过系统10%。

5.2.6 优化

a）客户端应对res资源进行优化，移除冗余文件，对图片等素材在使用效果可接受范围内进行压缩；

b）客户端应对dex进行优化，合理切分dex，类似代码功能尽量进行复用，去除不必要的冗余代码；

c）客户端应对lib组件进行优化处理，移除无关组件，对于不同功能模块共同使用的组件应进行合理复用。

5.3 移动金融客户端更新

移动金融客户端更新应满足基本要求：

a）客户端应通过正规的应用分发渠道发布，注明新版本的新特性说明；老的客户端版本可以收到更新提示或提供更新到新版本的入口；

b）新版本客户端发布前，应经过相关的功能、性能、安全评估测试，满足意思规范要求。

5.4 反欺诈

5.4.1 客户端环境、运行状况、操作行为监测

a) 金融机构应对客户端应用软件具备环境的检查能力，检查的范围应包括：系统是否越狱或root、程序运行环境是否可信等，并能向后台系统反馈设备环境信息等；

b) 金融机构应对移动金融客户端运行安全状况进行检测并向后台系统反馈，对设备的运行安全情况进行识别和监测，并建立相应的风控策略保障其客户端运行环境的安全性；

c) 针对移动金融客户端的用户行为进行监控，建立用户操作行为安全基线，实时预警用户不可控的行为，一旦发生预警，与客户主体进行联系，验证其客户身份及操作行为的真实性；

d) 应在门户网站或官方渠道发布移动金融客户端环境安全的提示。

5.4.2 仿冒钓鱼应用监测

金融机构应对移动应用市场进行7*24小时监测，及时发现仿冒手机银行的第三方移动应用。

5.4.3 设备运行环境可信监测

金融机构应对移动金融客户端用户环境风险进行监测，及时针对异常IP、地理位置、设备ID等多维度信息进行实时采集、预警、响应。

5.4.4 用户行为可靠监测

金融机构应对用户的交易行为进行事前、事中、事后的全过程监控，对异常交易行为进行威胁预警与风险策略保护。

5.4.5 欺诈人群信息监测

金融机构应充分利用内部以及外部公安涉炸、黑产及司法失信等信息，通过数据应用、数据获取与数据分析有效识别用户身份识别效率与准确度。

5.5 服务性能

5.5.1 易用性

手机银行移动金融客户端易用性应具备以下基本要求:

a) 以客户视角，宜提供客户账户总览、产品筛选、功能搜索、产品推荐等服务功能，使软件更简易、高效地适应用户的使用需求和习惯；
b) 宜提供语音导航方便客户使用；
c) 应在布局合理的情况下，做到输入简单，如提供图像识别自动录入卡面信息、粘贴板自动录入卡号信息等功能；
d) 业务流程应符合具体客户需求，最大程度减少操作步骤，使客户高效、直接完成功能操作；
e) 针对老年客群，应提供适老化服务，如支持切换“至简专版”服务。

5.5.2 易学性

应提供新手引导、新功能上线指引、在线客服，帮助客户快速学习功能使用方法。

5.5.3 舒适性

手机银行移动金融客户端舒适性应具备以下基本要求:

a) 宜采用统一的交互、视觉设计规范，信息表达简洁和美观；使用标准配色、合理运用色彩含义、色彩对比；
b) 提示文案应环境贴切，与现实匹配；应使用标准字体、字号；使用日常、自然的语言与用户进行交流；
c) 应融入情感化设计与用户进行情感交流，如有专属卡通形象作为与客户沟通纽带。

5.5.4 便捷性

手机银行移动金融客户端便捷性应具备以下基本要求:

a) 应做到功能易找，如支持客户定制页面内容及功能入口、常用功能前置、提供快捷金融小应用、交互层级扁平、栏目分类科学、导航清晰；
b) 操作所需步骤、流程应简洁有序，任务流程连贯闭环、无断点，功能具有接续性，反馈应友好、指引应清晰，如申请类、注册类服务有进度指示；
c) 应提供不同客群专属版本，如小微银行专版、私人银行专版；可根据服务客群，提供专属服务入口；
d) 宜提供线上线下一体化服务，如扫二维码支付、扫二维码取现、网点预约排号等服务；
e) 应提供丰富的生活周边服务，如生活缴费、网上购物、出行服务等服务。

5.5.5 易访问性

手机银行移动金融客户端易访问性应具备以下基本要求：

a) 客户端应支持主流应用商店下载、线下扫二维码下载等下载方式；
b) 移动银行端应具备指纹登录、手势登录、人脸登录等快捷登录方式；
c) 应提供客户端、WEB 浏览器、社交平台公众号等多种访问方式；
d) 银行网点宜提供自助服务终端，方便客户登录、下载、开通手机银行移动金融客户端；
e) 针对鸿蒙操作系统用户，应支持在鸿蒙操作系统上安装、适配、运行手机银行移动金融客户端。

5.5.6 稳定性

闪退率应≤0.05%。

6 创新与前瞻性

6.1 服务创新

6.1.1 创新机制

应规范中国民生银行创新管理工作，完善创新管理体系，提升自主创新能力，推动创新业务合规、有序、健康发展。移动金融聚焦客户服务体验，通过千人千面智能服务、金融产品的数字化创新、 IT 技术升级、业务流程改造等网络金融领域创新，提供前沿性、创新性的网络金融服务能力。应保障具备应用价值与较高的社会认可度。根据创新内容分为产品创新、模式创新、技术创新。

6.1.2 服务（产品）创新

产品创新包含以下内容：

a) 应使用统一用户体系，实现一套账户密码登录手机银行客户端、网银、信用卡全民生活客户端的等网络金融服务平台；
b) 针对不同客群的差异化服务需求，应提供面向专属客群的差异化版本服务能力；
c) 宜建设客户开放体系，实现对本行客户、他行客户、互联网客户的平台服务能力；
d) 宜提供远程视频服务，借助高速音视频传输、数据交互、身份识别等技术，为客户提供线上业务办理、线下物流实物交付、网点专人或移动上门服务支持和“端到端”服务流程跟进等全方位服务；
e) 应借助大数据分析，以智能化的方式区分个体差异，支持在多个版块及交易页面的广告区域、投资理财产品的推荐区域等千人千面精准营销，可根据客户属性（如地区、资产情况等）推送特色营销活动及个性化的产品；
f) 应根据个人客户个性化的风险偏好，实现根据交易时间、地点、金额、渠道等维度进行客户自定义的支付安全设置；
g) 应提供机器人智能应答服务，通过文字语意分析等技术，提供智能话术应答；
h) 宜将生物识别技术与手机银行移动金融客户端服务高度融合，为个人客户提供指纹支付和登录、人脸识别登录及转账、手势密码、虹膜支付等生物识别应用；
i) 宜将前沿性技术与手机银行移动金融客户端服务场景结合，提供语音识别、图像识别（OCR）等服务功能；
j) 聚合行内外内容资源，为客户提供风险防范、理财宣讲等非金融服务能力。

6.1.3 模式创新

模式创新包含以下内容：

a) 可通过 API 技术搭建开放银行服务平台，借助“嵌入场景、输出金融”的创新模式，实现将 II、III 类账户输出到合作商户，提供账户开立、账户管理、转账支付、财富产品、贷款产品等功能嵌入第三方；
b) 可提供信用卡虚拟化业务模式，实现线上实时申卡、办卡、激活等功能，支持虚拟卡实体化、无卡支付、消费及借贷的一站式用卡体验；

c） 可提供直销银行服务，通过提供在线 II、III 类账户服务和专属金融产品，客户全流程无需到网点办理，可以使用任何一家银行借记卡作为绑定账户，便捷地在线完成转账支付，购买投资理财产品，申请贷款等银行业务。

6.1.4 创新实践

手机银行移动客户端服务创新的具体案例包括以下内容：

a） 应响应国家“助力村振兴，实现共同富裕”战略目标，为“金融服务进县城、进乡村”业务模式的发展提供服务支撑。面向乡村客群，建设乡村专版，根据我国乡村基础条件和客群需求，提供具有乡村特色金融产品和服务，助力国家乡村振兴战略；

b） 应构建会员服务体系，丰富权益内容，面向全客群提供服务，实现对客户的长久陪伴；

c） 根据《国务院办公厅关于切实解决老年人智能技术困难实施方案的通知》（国办发〔2020〕45 号）、《银保监会办公厅关于银行保险机构切实解决老年人运用智能技术困难的通知》（银保监办发〔2021〕40 号）、《移动金融客户端应用软件无障碍服务建设方案》（银发〔2021〕69 号）的要求，为了弥合老年用户群体的数字鸿沟，我行推出手机银行长辈版专属服务，为老年及特殊群体提供全面贴心的移动金融服务。一方面，以功能精简、大字突出、交互简单、场景聚合为特色，覆盖手机银行主要功能包括转账、存款、缴费等。。二是开展无障碍软件客户端认证服务。我行已于 2022 年委托北京国家金融科技认证中心申请无障碍 APP 认证业务并于同年 12 月获《移动金融无障碍客户端软件认证证书》（无障碍等级三级）。

6.2 无障碍化使用

应确保创新产品无障碍使用，符合 GB/P37668 一 2019 中的要求，深化产品使用的可兼容性。

手机银行移动金融客户端无障碍化使用应具备以下基本要求：

a） 功能精简：以账户、转账、理财、储蓄及缴费等老年客群较为常用的功能为主；

b） 大字突出：视觉设计主要以清晰可辨为目标，应具备大字体、大图标、文字高对比度；

c） 交互简单：突出快捷登录、在线客服、服务搜索等功能，提供文本输入提示等功能；

d） 辅助功能：具备操作语音提示、自定义手势、首页功能自定义、关键词记录等功能；

e） 场景聚合：通过聚合各种适老化功能产品，为客户提供一体化场景服务，以非金融服务带动金融需求。

应考虑视力、听觉、行动及认知障碍等残障用户的产品使用需求，确保无障碍兼容性进行实时反馈联络。在操作流程中，应为残障用户留出充足的操作时间，应支持屏幕阅读器和操作辅助工具开启时，功能性组件应均能正常使用。

6.2.1 可感知性

6.2.1.1 非文本处理

6.2.1.1.1 色彩体系

色彩体系在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a） 应构建完整的色彩体系，规范、统一应用的背景色、主色、辅色、控件色彩、数据表达色、栏目色等内容，确保用色的一致性；

b） 应通过运用图形的色彩含义及合理对比度有效划分功能层级关系，快速引导用户使用这些功能并完成任务；

c） 应将主色彩（红色）用于产品界面的重要功能中，主色彩应固定唯一且使用准确；该色彩主要用于需要强调和突出的文字按钮，包括但不限于：用于提示重点操作、引导性操作以及重要的内容信息；

d） 应将辅助色广泛应用于产品的信息内容，色彩依据信息优先级采用不同的明度，以达到正确引导用户完成任务的目的；

e） 应遵循文本重要内容深色，次要内容浅色，相同场景、功能内容采用同一色号的原则。

6.2.1.1.2 图标

图标在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a） 图标应整体风格统一，通过主形和辅助形结合的方式阐明语义；

b） 应具有辨识性，以达到帮助用户区分和理解不同产品和功能的目的；

c） 应确保图形易理解，即能够让用户一望而知；

d） 应确保图形易再认，即做到容易记忆，即使用户不能马上理解，也能够在再次使用时认出来，具有辨识性；

e） 应确保图形易区分，即应能够在其他图标中被区分出来。

6.2.1.2 文本处理

6.2.1.2.1 颜色用途

颜色用途在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在客户端应用软件中，应确保文本颜色不是传达信息、表明动作、提示响应等区分视觉元素的唯一手段。

6.2.1.3 信息反馈

6.2.1.3.1 提供完整的信息反馈方式

提供完整的信息反馈方式在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a） 在用户用于理解内容和操作内容的表现方式或操作上，不应单独依赖于组件的感观特性，如组件的形状、大小、方向、声音或视觉位置；

b） 在用户进行一项操作后，应立即有一个与之相对应的反馈呈现给用户，使用户能够确认自己的操作；

c） 在用户输入信息过程中，产品应结合使用场景，智能地提供与用户输入相关联的提示；

d） 在对于操作页面元素带来的变化和页面之间的转场，适当地加入一些过渡动效，以保持视觉的连贯性，帮助用户理解页面之间和页面元素之间的逻辑关系；

e） 在用户的操作不能立刻完成时，为用户反馈任务的处理进度，避免让用户失去等待的耐心和对产品的信心。

6.2.1.3.2 文案组织形式

文案组织形式在满足GB/T37688-2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a） 应时刻保持服务意识，带着情感和温度跟用户进行对话，让用户体验会到贴心的服务态度；

b） 应用自信和肯定的语气赢得用户的信赖，使用户产生安全感和信赖感；

c） 应给予用户友好平等的感觉。像用户的朋友一样去对待用户所遇到的困难或问题，给予帮助和支持；

d） 在进行提示时，应准确描述当前情况并告知相应解决方案。不应出现报错信息代码或过于专业的描述。

6.2.2 可操作性

6.2.2.1 布局访问

6.2.2.1.1 功能性组件访问

功能性组件访问在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在客户端应用软件中，所有可见的非装饰性组件均应被辅助工具正常访问。在页面局部更新后，不可见的组件应不可访问，新出现的可见非装饰性组件应能被用户及用户代理正常访问。

6.2.2.1.2 装饰性内容访问

装饰性内容访问在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在客户端应用软件中，所有可见的纯装饰性内容均应被辅助工具主动忽略。

6.2.2.2 操作控制

6.2.2.2.1 悬浮窗

漂浮窗在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a) 应提供可访问或可关闭的操作机制；
b) 应确保不会遮挡、干扰主要操作；
c) 应充分考虑内容与样式的契合度，在符合页面整体风格的前提下，漂浮窗样式可与其内容呼应。

6.2.2.2.2 手势操作

手势操作在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a) 在客户端应用软件中，应对用户进行手势导航或者对操作的结果进行反馈提示；在开启无障碍功能服务时，原有手势操作仍能工作；如果失效，则应提供相应的替代操作方式，例如通过音量加减键控制；
b) 在移动端中，应包括但不限于点击、拖拽、滑动、轻扫、双击、捏合、长按、摇晃及其他形式；
c) 点击手势，应用于包括但不限于以下应用场景：确认、下一步、选择、取消选择；
d) 滑动手势，应为在页面中点中、快速滑动、提起的动作，包括但不限于以下应用场景：在页面中进行滑动并刷新当前页面，展现更多功能；
e) 轻扫手势，应为在页面中为了快速删除或编辑某项功能，点中选项向左轻扫的动作，包括但不限于以下应用场景：在页面中使用轻扫出现删除按钮，点击可删除；
f) 双击手势，应为在页面中连续两次点击屏幕，放大或缩小图片内容的动作，包括但不限于以下应用场景：在地图中双击任一点，放大地图；
g) 捏合手势，应为在页面中双指张开或捏合的动作，包括但不限于以下应用场景：在地图中使用捏合动作，放大查看地图；
h) 摇晃手势，应为在页面中摇晃设备呼出隐藏菜单或进行撤销操作的动作，包括但不限于以下应用场景：摇晃设备呼出“摇一摇”菜单。

6.2.2.2.3 闪光

闪光在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a) 考虑到无障碍设计的需要，应保障闪光等光学元素的运用（如闪光、特殊光颜色）的阈值区间涵盖特殊人群需求；
b) 不应包含闪光超过 3 次每秒的内容，或闪光低于一般闪光和红色闪光阈值。

6.2.2.2.4 焦点顺序

焦点顺序在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在客户端应用软件中，如过界面可以进行顺序导航，且导航顺序影响含义和操作，则可聚焦元素应以保持其含义和可操作的顺序获取焦点。

6.2.2.2.5 弹出干扰

弹出干扰在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a） 对于悬停或焦点上显示的信息内容，应能关掉或确保不会掩盖触发内容；

b） 应确保弹出的信息内容不会打断流程或造成操作中断；

c） 提示信息应简洁清晰。

6.2.2.2.6 更新提示

更新提示在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a） 已阅读过的内容模块有更新时，应通过某种机制向用户传达已更新的通知；

b） 提示可为应用内提示，也可为系统或其他渠道的提示；

c） 提示应简明易懂，确保可以快速获取重点信息；

d） 应有可访问或可关闭的操作机制；

e） 可包含但不限于以下辅助元素：图片、链接、动效。

6.2.2.2.7 单键式快捷键

单键式快捷键在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足如果仅使用字母（包括大写和小写字母）、标点符号、数字或符号字符在内容中实现键盘快捷键，则应至少满足下列条件之一：

a） 关闭：有一种机制可以关闭快捷方式；

b） 重定向：使用一种机制重新定义快捷方式以使用一个或多个键盘字符；

c） 仅在焦点上有效：组件的键盘快捷键仅在该组件具有焦点时才处于活动状态。

6.2.2.2.8 充足的操作空间

操作时间在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在客户端应用软件中，如果显示不是活动的必要部分或关键要素，且不会导致用户发生法律承诺或财务交易，则应为用户的操作留下充足时间，在用户操作完毕前不发生变化。

6.2.2.3 信息输入处理

6.2.2.3.1 并发输入机制

并发输入机制在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在客户端应用软件中，不应限制使用平台上可用的输入模式，但当需要确保内容的安全性或尊重用户设置的情况下除外。

6.2.3 可理解性

6.2.3.1 信息内容处理

6.2.3.1.1 不常用词语

不常用词语在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a） 在客户端应用软件中，所有可见的非装饰性组件均应被辅助工具正常访问。在页面局部更新后，不可见的组件应不可访问，新出现的可见非装饰性组件应能被用户及用户代理正常访问；

b） 在客户端应用软件中，所有可见的纯装饰性内容均应被辅助工具主动忽略；

c） 在客户端应用软件中，如果显示不是活动的必要部分或关键要素，且不会导致用户发生法律承诺或财务交易，则应为用户的操作留下充足时间，在用户操作完毕前不发生变化。

6.2.3.1.2 缩写词

缩写词在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足若文案中存在缩写词，应提供小i等一定机制来确定缩写词的展开形式或含义，且该机制可正常使用。

6.2.4 内容一致性

6.2.4.1 聚焦稳定

聚焦稳定在满足GB/T37668—2019中相关指标的三级要求基础上，在任何组件被聚焦时，不应引起上下文变化。

6.2.4.2 一致的布局

一致的布局在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a) 界面风格应保持一致，在多个界面重复出现的元素应采用一致的布局；
b) 在多个界面出现的相同模块应采用一致的布局；
c) 同种类型控件对齐方式应保持一致。

6.2.5 帮助信息

6.2.5.1 错误原因提示

错误原因提示在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在用户输入错误信息时，应能被自动检测出错误所在并以文本等形式向用户描述错误原因。

6.2.5.2 错误原因修改建议

错误原因修改建议在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在用户输入错误信息时，应能被自动检测出错误所在并以文本等形式向用户提供修改建议。

6.2.5.3 错误预防

错误预防在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a) 在用户完成录入和选择操作时，在最后提交前，应提供一个检查、确认、修改信息的机制；
b) 在用户进行容易发生错误或有风险的操作时，应额外设置一些操作障碍或对操作提出限制性要求，以减少失误；
c) 在用户进行较为复杂的操作时，可以为用户提供与当前操作相关的合理建议，以帮助用户理解和掌握使用条件，若难以通过设计手段限制用户操作时，可采用简短的文字提示告知用户操作时的注意事项；
d) 在用户进行输入操作时，应提供可逆的撤销操作。

6.2.6 兼容性

6.2.6.1 无障碍兼容性

6.2.6.1.1 辅助性组件功能

辅助性组件功能在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足辅助工具开启时，客户端应用软件内容中所有功能性组件均能正常工作；可见链接能正常跳转；按钮可正常访问；输入框能正常输入；多媒体能正常播放；在无法按原状态工作情况下，应提供等效的方法继续完成功能工作。在页面局部更新后，客户端应用软件内容中新增的功能性组件也应能正常工作。

6.2.6.1.2 整体体验连贯性

整体体验连贯性在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下具体要求：

a) 应确保同一产品在不同渠道的基本流程保持一致；
b) 应在同一渠道同类或相似场景中采用一致的交互方式；

c) 应对同一渠道产品中功能相似或逻辑关联性较强的产品界面，采用统一的界面布局与视觉进行设计。

6.2.6.2 用户交融兼容性

6.2.6.2.1 用户反馈联络

用户反馈联络在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在为用户提供支持服务入口时，应支持不同类型人群的使用，以满足不同用户个性化的需求。

6.2.6.2.2 实时用户反馈联络

实时用户反馈联络在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足在网站中所预留的联系方式中，应支持不同类型人群的使用，以帮助用户能够完成后续的基于互联网的、实时的交互操作。

6.2.7 适老化功能实现要求

适老化功能实现要求在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下要求：

a) 在辅助工具开启时，应保证应用内容中所有功能性组件均能正常工作：按钮可正常访问；输入框能正常进行输入；多媒体能正常播放；在页面局部更新后，移动应用内容中新增的功能性组件也应能正常工作；

b) 内嵌适老版界面的应用首页需具备显著入口，支持切换至适老版，或在首次进入时给予显著切换提示，且在“设置”中提供“长辈版”入口；具备搜索功能的应用应将“长辈版”作为标准功能名，用户可通过搜索功能直达，同时设置“亲情版”、“关爱版”、“关怀版”等别名作为搜索关键字。

6.2.8 鸿蒙系统功能实现要求

鸿蒙系统功能实现要求在满足GB/T37668—2019中相关指标的三级要求基础上，应同时满足以下要求：

a) 应确保在不同终端设备之间的极速连接、能力互助、资源共享，匹配合适的设备、提供流畅的全场景体验；

b) 应充分了解所要支持的设备，包括屏幕尺寸、交互方式、使用场景、用户人群等，对设备的特性进行针对性设计，还需要考虑不同设备的共性，保证跨设备的一致性，从而减少用户学习的难度，降低应用开发成本；

c) 应考虑多个设备之间的多种相互协同模式，最大程度展现鸿蒙系统上独特的多设备无缝流转体验。

6.3 技术前瞻

6.3.1 技术创新内容

技术创新包含以下内容：

a) 针对互联网级别的海量客户、海量服务、海量数据，应在基础架构上进行分布式架构转型并商用于核心生产系统；

b) 应使用大数据技术，包含但不限于：风险与欺诈分析、运营优化、市场洞察、舆情分析、智能获客等方面；

c） 可使用指纹、人脸、虹膜等生物识别技术认证方式，增强身份认证安全性和认证手段多样性，若采用生物特征识别作为验证要素，应当符合国家、金融行业标准和相关信息安全管理要求，取得客户的单独同意，防止非法采集、存储、复制和使用生物特征数据。
d） 根据客户端环境，可同时支持 FIDO 指纹特征识别和人脸特征识别，FIDO 指纹特征识别主要用于移动金融客户端交易环境认证，人脸特征识别用于实人认证；
e） 宜建设自然语言处理平台，向手机银行等移动端服务平台提供服务支撑；
f） 宜实施基础设施 SaaS 云化改造和容器云 PaaS 建设，宜推进移动金融相关应用云端化。

6.3.2 技术创新实践

民生银行基于分布式技术，完成了银行核心系统的无缝升级改造，基于大数据风控模型，在转账、贷款、支付等业务场景增加了业务风险处置，在端侧增加了威胁感知能力。综合应用指纹、人脸、虹膜等生物识别技术，以及短信、sim 卡认证等技术，在渠道侧形成了可根据具体业务进行灵活配置的安全验证工具。

7 实施保障

7.1 组织机构保障

7.1.1 手机银行移动金融客户端业务牵头部门

手机银行移动金融客户端业务牵头部门的具体职能包括：
a） 统筹管理全行手机银行移动金融客户端业务，制定和组织实施我行手机银行移动金融客户端业务发展规划；
b） 负责手机银行移动金融客户端各类渠道服务的统一管理；
c） 负责手机银行移动金融客户端业务统一的需求统筹、平台建设、敏捷开发、流程管理、风险管理、数据挖掘、营销策划等；
d） 负责手机银行移动金融客户端业务管理、制度建设、监管报批、安全建设、反洗钱等职责。

7.1.2 手机银行移动金融客户端支持保障部门

手机银行移动金融客户端支持保障部门的具体职能包括：
a） 应由信息科技部门负责信息科技建设管理体系规范，负责手机银行移动金融客户端业务相关系统建设管理及运营维护工作；
b） 应由运营管理部门负责手机银行移动金融客户端柜面业务相关的账户管理、资金清算、账务处理、客户服务的操作流程制定与管理、后台业务集中运营等；
c） 应由审计部门负责对全行手机银行移动金融客户端业务进行相关审计；
d） 应由零售、金融市场等业务条线部门负责各自领域的产品线上化管理。

7.1.3 分行机构

分行应贯彻落实总行手机银行移动金融客户端业务发展规划和工作部署，执行各项手机银行移动金融客户端业务管理制度，组织开展手机银行移动金融客户端产品推广、市场拓展、业务检查、安全教育、同业调研等工作，配合总行开展风险事件协查处理。

7.2 管理制度

7.2.1 产品研发类制度

应制定产品研发类制度，以确保手机银行移动金融客户端相关的产品研发资源合理安排，规范研发项目的管理流程，提高研发效率，具体包括：产品创新制度、项目评审制度、项目管理制度，项目开发规范、设计规范、后评估机制等。

7.2.2 测试投产类制度

应制定测试投产类制度，以确保手机银行移动金融客户端相关的项目安全、高效、顺利实施，具体包括：测试过程管理规范、测试质量管理规范、系统投产规范等。

7.2.3 生产运维类制度

应制定生产运维类制度，以确保手机银行移动金融客户端相关的生产安全与运维规范，具体包括：生产运维规范、配置规范、变更规范，以及系统、网络、机房、数据、安全等配套管理规定。

7.2.4 业务管理类制度

手机银行移动金融客户端业务应制定业务管理办法，以规范其部门职责、业务范围、经营模式、风险管理等。手机银行移动金融客户端提供的各类线上业务应遵循相关产品负责部门提供的产品管理办法，包括但不限于转账汇款、支付缴费、存款类、贷款类、投资交易类等。

7.2.5 应急响应类制度

应制定应急响应类制度，以确保手机银行移动金融客户端业务具备应急响应措施，妥善处理各类突发事件，保证业务的连续性，具体应包括：信息系统、反洗钱、流动性、消费者权益保护等突发事件应急预案、业务连续性应急预案、生产系统事件管理办法等。

7.3 企业标准宣传及实施机制

7.3.1 宣传与培训机制

应确定企业标准的管理部门，建立总行、事业部、分行的分层宣传与培训机制，确保层层传导。

全行各级机构应针对标准定期组织开展多层次的业务培训和文化建设活动，提升相关人员的专业知识和标准服务意识。

全行各级机构应认真学习企业标准，管理部门应对各部门进行业务培训，有条件的宜进行考试及认证工作，按要求落实企业标准要求。

应将企业标准上传公示至标准信息公共服务平台，并将企业标准纳入行内广告投放与宣传的计划范围内。

7.3.2 实施监督机制

全行各级机构应制定贯彻落实企业标准的工作机制，建立严格的实施监督制度，各级机构可将企业标准分解指标，纳入相关团队的考核。

全行各级机构应将对企业标准的执行情况定期上报，企业标准的管理部门应对各机构情况进行汇总和通报，对出现不符合标准的情况，应及时督导整改。

企业标准的管理部门应根据行内业务实际的发展情况，每年对标准进行维护和更新，并将最新版的标准进行公示和行内发布。

参 考 文 献

[1]GB/T 32315—2015　银行业客户服务中心基本要求
[2]GB/T 29799—2013　网页内容可访问性指南
[3]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