Q/HRBB

哈尔滨银行股份有限公司企业标准

Q/HRBB 001—2025

哈尔滨银行移动金融客户端应用规范

Financial mobile application software application specification of Harbin Bank

2025-12-08 发布　　2025-12-08 实施

哈尔滨银行股份有限公司 发布

目　次

前　言

本标准按照 GB/T 1.1—2020 给出的规则起草。

本文代替 Q/HRBB 001—2024《哈尔滨银行移动金融客户端应用规范》，与 Q/HRBB 001—2024 相比主要变化为：

1、更新 5.3 发布要求

2、更新 6.5.3 缺陷解决时间

3、更新 7.1 兼容性

4、更新 7.2 性能

5、更新 7.3 移动金融客户端更新

本文件由哈尔滨银行股份有限公司提出并归口。

本文件起草单位：哈尔滨银行股份有限公司。

本文件主要起草人：孙伟超、曹琦、吴学敏、罗进、郭彪、陈奇伟、王宇川、刘颖杰。

哈尔滨银行移动金融客户端应用规范

1 范围

本标准规定了哈尔滨银行向客户提供手机银行等移动金融客户端的功能要求、系统安全技术要求、安全管理要求、业务运营安全要求。

本标准适用于哈尔滨银行手机银行等移动金融客户端服务。

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 27912—2011 金融服务生物特征识别安全框架

GM/T 0021—2012 动态口令密码应用技术规范

GB/T 35273-2020 信息安全技术 个人信息安全规范

JR/T 0071 金融行业网络安全等级保护实施指引

JR/T 0098.5 中国金融移动支付 检测规范 第5部分：安全单元（SE）嵌入式软件安全

JR/T 0118—2015 金融电子认证规范

JR/T 0149—2016 中国金融移动支付支付标记化技术规范

JR/T 0156—2017 移动终端支付可信环境技术规范

JR/T 0092—2019 移动金融客户端应用软件安全管理规范

JR/T 0068—2020 网上银行系统信息安全通用规范

JR/T 0171-2020 个人金融信息保护技术规范

中国人民银行关于改进个人银行账户服务加强账户管理的通知（银发〔2015〕392号），2015-12-25

中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号），2016-06-13

中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知（银发〔2016〕261号），2016-09-30

中国人民银行关于落实个人银行账户分类管理制度的通知（银发〔2016〕302号），2016-11-25

中国人民银行办公厅关于强化银行卡磁条交易安全管理的通知（银办发〔2017〕120号），2017-05-31

条码支付安全技术规范（试行）（银办发〔2017〕242号文印发），2017-12-22

中国人民银行关于改进个人银行账户分类管理有关事项的通知（银发〔2018〕16号），2018-01-10

中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知（银发〔2019〕85号），2019-03-22

3 术语和定义

3.1

移动终端 mobile terminal

区别于PC机方式，以手机、平板电脑、可穿戴设备等访问网上银行的移动设备。

3.2

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。

3.3

资金交易类移动金融客户端应用软件 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。

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。

4 基本安全要求

4.1 身份认证安全

4.1.1 认证方式

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）移动金融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，如：对于大额资金交易，移动金融客户端应采用两种或两种以上要素对用户身份进行认证等。

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）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；
2）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；
3）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。

e）若采用图形验证码作为验证的辅助要素，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，移动金融客户端源文件中不应包含图形验证码文本内容。

f）图形验证码不得作为独立的身份验证要素。

增强要求应符合 JR/T 0092-2019 中 5.1.1 的增强要求。

4.1.2 认证信息安全

4.1.2.1 安全输入

移动金融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，移动金融客户端应提供以下安全控制措施，或其他经攻击测试无法获取明文的安全防护措施。

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。

增强要求应符合 JR/T 0092-2019 中 5.1.2.1 的增强要求。

4.1.2.2 个人金融信息展示

a) 移动金融客户端应用软件的口令框应默认屏蔽显示，屏蔽显示时应使用同一特殊字符（例如*或•）代替。

b) 移动金融客户端应用软件不应明文显示银行卡密码和网络支付交易密码。

c) 移动金融客户端应用软件展示个人金融信息时，应符合以下要求：

1) 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）；

2) 处于已登录状态时，个人金融信息展示的技术要求如下：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等可以直接或组合后确定信息主体的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，应履行移动金融客户端身份验证，并做好此类信息管理，防范此类信息泄露风险；涉及其他信息主体的信息时，宜进行屏蔽展示，当满足如下条件之一时可不脱敏：其他方主动发起的活动包含的信息，如其他方发起交易、收付款；与其他方已建立信任关系（间接授权），如向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人。

4.1.3 认证失败处理

a) 移动金融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) 移动金融客户端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。

4.1.4 密码的设定与重置

a) 移动金融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。

b) 移动金融客户端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密码。

c) 移动金融客户端在修改密码前，应对用户身份进行重新验证。

d) 移动金融客户端修改密码时应对原密码输入错误次数进行限制。

e）移动金融客户端修改密码时新密码不应与原密码相同。

f）移动金融客户端在密码重置时，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。

4.2 逻辑安全

4.2.1 逻辑安全设计

a）移动金融客户端对于认证、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）移动金融客户端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。

4.2.2 软件权限控制

移动金融客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。

4.2.3 风险控制

a）移动金融客户端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）移动金融客户端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）移动金融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。

4.2.4 回退处理

移动金融客户端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。

4.2.5 异常处理

a）移动金融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。

4.3 安全功能设计

4.3.1 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移动金融客户端应用软件信息和个人信息。

4.3.2 接口安全

a） 移动金融客户端软件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） 移动金融客户端软件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。

4.3.3 抗攻击能力

a） 移动金融客户端软件应用软件应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） 移动金融客户端软件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） 移动金融客户端软件应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。

d） 移动金融客户端软件应用软件如使用安全输入控件，该控件应具备抵御一定程度攻击的能力。

增强要求应符合JR/T 0092-2019中5.3.3的增强要求。

4.3.4 移动金融客户端应用软件环境检测

移动金融客户端应用软件在运行时应具备对运行环境的检查能力，检查的范围可包括：系统是否被未经授权获取管理员权限、程序运行环境是否可信（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信息等。

4.4 密码算法及密钥管理

4.4.1 密码算法

a） 移动金融客户端软件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。

4.4.2 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。

4.5 数据安全

4.5.1 数据获取

4.5.1.1 数据防窃取

a） 移动金融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） 移动金融客户端应用软件的临时文件中不应出现支付敏感信息，临时文件包括但不限于Cookies、本地临时文件等。

c） 移动金融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） 移动金融客户端应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文。

增强要求应符合 JR/T 0092-2019 中 5.5.1.1 的增强要求。

4.5.1.2 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，应采取防篡改机制保证数据不被移动终端的其他程序篡改。

4.5.1.3 数据有效性

移动金融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。

4.5.2 数据访问控制

a） 应采取措施保护移动金融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。

b） 移动金融客户端软件应用软件在授权范围内，不应访问非业务必需的文件和数据。

4.5.3 数据传输

4.5.3.1 通讯安全

a） 应在移动金融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） 移动金融客户端软件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。

4.5.3.2 数据保密性

a） 敏感数据（如：登录口令、支付敏感信息等）在客户端应用软件与本地其他应用软件间传输时，应采取加密等措施确保其保密性，若本地其他应用软件不能提供与移动金融客户端应用软件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。

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。

4.5.3.3 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（如：数字签名、MAC 等）确保其完整性，若本地其他应用软件不能提供与金融移动金融客户端软件相应等级的数据完整性保护措施，则应评估关键数据传输的风险，并设计补救措施。

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（如：数字签名、MAC 等）确保其完整性。

4.5.3.4 数据抗抵赖

通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术。

4.5.3.5 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，应能够防止重放攻击。

4.5.4 数据存储

4.5.4.1 个人金融信息存储

a） 移动金融客户端软件应用软件不应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。

b） 在满足法律、管理规定的前提下，客户端应用软件应仅保存业务必需的个人金融信息，并限制数据存储量。

4.5.4.2 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。

4.5.5 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。

4.5.6 数据销毁

4.5.6.1 残余信息保护

a） 移动金融客户端软件应用软件应在敏感数据使用完毕后，对其立即进行清除。

b） 移动金融客户端软件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） 移动金融客户端软件应用软件卸载完成后，文件系统中不应残留任何个人金融信息。

增强要求应符合 JR/T 0092-2019 中 5.5.6.1 的增强要求。

4.5.6.2 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。

增强要求应符合 JR/T 0092-2019 中 5.5.6.2 的增强要求。

4.5.6.3 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 应用软件管理要求

5.1 设计要求

a） 移动金融客户端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。

b） 移动金融客户端软件应提供易用、风格统一、体验良好的用户界面。

c） 移动金融客户端软件应遵循合法、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。

d） 移动金融客户端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。

e） 移动金融客户端软件不得以默认、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。

增强要求应符合 JR/T 0092-2019 中 6.1 的增强要求。

5.2 开发要求

a） 移动金融客户端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） 移动金融客户端软件开发过程中应建立并维护开发文档。

c） 移动金融客户端软件开发完成后，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） 移动金融客户端软件的每次重要更新、升级，都必须经过严格的开发流程规范、归档、源代码扫描、发布审核、规定执行等步骤。

5.3 发布要求

a） 客户端应用软件应有规范的上线发布流程，由应用软件的所有方对应用软件进行签名和保护，标识应用软件的来源和发布者，提供安全可靠的应用软件下载、发布、升级渠道。

b） 移动金融客户端软件应当删除调试或测试中存留的敏感数据。

c） 移动金融客户端软件安装过程中，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。

d） 移动金融客户端软件有新版本时，不得未经用户允许自动安装新版本，但不包括安卓、iOS 和 HarmonyOS 系统的用户在设置中开启了软件自动更新的情况。

e） 若移动金融客户端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。

5.4 维护要求

a） 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。

b） 移动金融客户端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。

c） 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 安全性要求

6.1 个人信息安全

6.1.1 收集

a） 移动金融客户端软件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） 移动金融客户端软件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。

增强要求应符合 JR/T 0171-2020 中 6.1.1 和 GB/T 35273-2020 中 5 的要求。

6.1.2 传输

a） 应建立相应的个人信息传输安全策略和规程，采用满足个人信息传输安全策略的安全控制措施，如安全通道、数据加密等技术措施。

b） 传输个人信息前，通信双方应通过有效技术手段进行身份鉴别和认证。

c） 应根据个人金融信息的不同类别，采用技术手段保证个人信息的安全传输；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全传输保障手段。

e） 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。

f） 应建立有效机制对个人金融信息传输安全策略进行审核、监控和优化，包括对通道安全配置、密码算法配置、密钥管理等保护措施的管理和监控。

g） 应采取有效措施（如个人金融信息传输链路冗余）保证数据传输可靠性和网络传输服务可用性。

增强要求应符合 JR/T 0171-2020 中 6.1.2 的 C3 类数据传输要求。

6.1.3 存储

a） 应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的存储安全；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全存储保障手段。

b） 不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。

c） 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中的安全性。

d） 应将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储，确保去标识化、匿名化后的信息与个人金融信息不被混用。

e） 在停止运营时，应依据国家法律法规与行业主管部门有关规定要求，对所存储的个人金融信息进行妥善处置，或移交国家与行业主管部门指定的机构继续保存。

6.1.4 使用

a） 移动金融客户端软件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） 移动金融客户端软件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） 移动金融客户端软件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） 移动金融客户端软件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） 移动金融客户端软件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） 移动金融客户端软件应允许用户关闭定向推送信息功能；

g） 移动金融客户端软件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） 移动金融客户端软件应向用户提供撤回同意收集个人信息的途径、方式；

i） 移动金融客户端软件应遵守声明的收集使用规则收集使用个人信息；

j） 移动金融客户端软件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） 移动金融客户端软件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） 移动金融客户端软件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） 移动金融客户端软件收集个人信息的频度等不应超出业务功能实际需要；

n） 移动金融客户端软件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） 移动金融客户端软件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移动金融客户端软件的使用。

增强要求应符合 JR/T 0171-2020 中 6.1.4 的 C3 类数据使用要求。

6.1.5 删除和销毁

a） 移动金融客户端软件应提供有效的更正、删除个人信息及注销用户账号功能；

b） 移动金融客户端软件应为更正、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） 移动金融客户端软件应提供更正、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移动金融客户端软件应和相应服务端后台共同完成；

e） 移动金融客户端软件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。

6.2 身份认证信息

a） 交易密码复杂度应符合以下要求：

1） 不可设置为重复的单一数字，如 111111 等；

2） 不可设置为连续数字，如 123456 等；
3） 不可设置为身份证号中任意截取的 6 位；
4） 不可设置为与登录密码相同。

b） 设备认证：客户更换设备使用 APP 时必须进行设备绑定，并且绑定需要进行双因素校验。

6.3 密码安全

6.3.1 密码应用方案制定

移动金融客户端应用软件与系统之间的数据传输机密性指标，应使用国产密码保证重要数据在传输过程中的机密性，密码应用方案应以对资金有关交易或重要业务操作进行保护为基础，在此之上从机密性、完整性、真实性、不可否认性、易用性等多方面进行考虑。具体要求需符合 GB/T 39786-2021 中 8.4 的要求，增强要求需符合 GB/T 39786-2021 中 9.4 的要求。

6.3.2 密码算法选择

根据应用场景应从国产密码算法 SM2、SM3、SM4 中进行选择。

6.3.3 密码策略应用

密码策略应符合以下要求：

a） 移动金融客户端应用软件与服务端采用单项国密 SSL（版本 SM2v1.1）通讯
b） 密码套件应选择 ECC-SM4-SM3 和 ECDHE-SM4-SM3。

6.3.4 密码安全性评估

依据《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》的三级系统要求，通过部署 SSL 中间件及国密应用安全网关，需符合如下评估项：

a） 网络和通信安全：
1） 部署应用安全网关，建立安全的数据传输通道确保数据的完整性。
2） 部署应用安全网关，建立安全的数据传输通道，确保数据的完整性。
3） 应用安全网关中实现密码算法、密码技术、密钥管理。

b） 应用和数据安全
1） 部署应用安全网关，建立安全的数据传输通道，确保数据以国密 SSL 通道加密的方式实现传输机密性。
2） 部署应用安全网关，建立安全的数据传输通道，确保数据以国密 SSL 通道加密的方式实现传输完整性。
3） 由应用安全网关实现密码算法、密码技术、密码服务、密钥管理。

6.4 风险提示

a） 移动金融客户端应用软件切换到后台时应进行风险提示；
b） 移动金融客户端应用软件在监测到 Root、越狱等设备时应进行风险提示；
c） 移动金融客户端应用软件在监测到可疑、异常交易时应进行风险提示；
d） 移动金融客户端应用软件在监测到摄像头劫持检测时应进行风险提示；
e） 移动金融客户端应用软件人脸认证时监测到照片、换脸、面具、遮挡以及屏幕翻拍时应进行风险提示。

6.5 缺陷解决率

6.5.1 缺陷分级

a） 致命缺陷：致命的错误，造成系统崩溃、死机，或造成数据丢失、主要功能完全丧失等。

b） 严重缺陷：严重错误，指功能模块或特性没有实现，主要功能部分丧失，次要功能全部丧失，或致命的错误声明。

c） 一般缺陷：不太严重的错误，如次要功能模块丧失、提示信息不够准确、用户界面差和操作时间长等。

d） 轻微缺陷：一些小问题如有个别错别字、文字排版不整齐等，对功能几乎没有影响，系统仍可正常使用，且对业务流程无影响。

6.5.2 缺陷解决率

缺陷解决率应符合以下要求：

a） 致命缺陷：系统上线前不允许有致命缺陷，即解决率应为 100%。

b） 严重缺陷：系统上线前不允许有严重缺陷，即解决率应为 100%。

c） 一般缺陷：系统上线允许有少量一般缺陷，但一般缺陷解决率应≥90%。

d） 轻微缺陷：系统上线允许有少量一般缺陷，但轻微缺陷解决率应≥85%。

6.5.3 缺陷解决时间

在不包括移动金融客户端需要 App Store 及安卓和 HarmonyOS 应用市场审查等原因的前提下，缺陷解决率时间应符合以下要求：

a） 致命缺陷：上线后的致命缺陷解决时间应在 4 小时内。

b） 严重缺陷：上线后的严重缺陷解决时间应在 4 小时内。

c） 一般缺陷：上线后的一般缺陷解决时间应在 5*24 小时内。

d） 轻微缺陷：上线后的轻微缺陷解决时间应在 30*24 小时内。

7 技术先进性要求

7.1 兼容性

随着机型、操作系统及涉及到 SDK 集成的需求迭代升级，系统软件的兼容性应进行及时更新，应符合以下要求：

a） 移动金融客户端软件兼容终端型号数量需≥600；

b） 移动金融客户端软件运行支持的操作系统最低版本:安卓 4.4.1 及 iOS9；

c） 移动金融客户端软件运行支持的操作系统：安卓、iOS 和 HarmonyOS；

d） 移动金融客户端软件需支持 IPv6 网络环境。

7.2 性能

a） 安装包大小应进行必要的优化，在不集成新业务、技术相关 SDK 前提下，移动金融客户端软件安装包文件大小需满足以下要求:

1) 安卓安装包大小不超过 520MB，iOS 安装包大小不超过 400MB，HarmonyOS 安装包大小不超过 350MB，安装后大小不应超过 600MB；
2) res 资源文件应进行必要的优化，去掉冗余文件，并合理使用对应质量的资源文件；
3) dex 文件应进行必要的优化，去掉冗余代码，并且尽量去掉调试信息等内容；
4) lib 文件应进行必要的优化，去掉冗余文件，并尽量减少非必要的 so 文件。

b） 移动金融客户端软件后台服务器的平均响应时间不应超过 1 秒，但服务器硬件设备、运营商、接入三方服务的请求发生异常情况下除外。

c） 应用不占用过多的内存资源，能及时释放内存，避免内存泄漏。

7.3 移动金融客户端更新

a） 移动金融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。

b） 移动金融客户端应用软件更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。

c） 移动金融客户端应用软件应支持 H5 和 Vue 页面动态补丁更新。

7.4 反欺诈

a） 移动金融客户端应用软件应配合后台 AI 算法反欺诈服务，在照片、换脸、面具、遮挡以及屏幕翻拍时做出相应提示和功能限制。

b） 移动金融客户端应用软件应进行 Root、越狱检测，并进行相应提示和功能限制。

c） 移动金融客户端应用软件应进行摄像头劫持检测，并进行相应提示和功能限制。

d） 移动金融客户端应用软件应配合后台基于业务策略规则，对于可疑交易，进行相应提示和功能限制。

8 创新及前瞻性要求

8.1 服务创新

移动金融客户端应用软件应进行适老化及无障碍设计，具体要求如下：

a） 视觉设计简约、温馨、清晰：
   1） 应减少装饰元素使用，降低页面干扰；
   2） 应以暖色系为主，传递温馨、温暖的视觉感受；
   3） 临近色彩对比度符合 WCAG 规定，普遍在 4.5:1；在字体颜色使用时减少灰色，拉开颜色对比度；
   4） 应使用“8 像素”原则，使页面间距更加统一规范。

b） 功能设计易用、智能：
   1） 应简化功能，直接展示快捷功能入口，避免业务无关入口干扰；
   2） 应设置“一键帮助”，提供在线客服、一键打电话客服、语音导航功能帮助用户解决问题；
   3） 应设置一键操作，文本输入设置引导性文案、输入联想等帮助用户提升操作效率；
   4） 快速转账支持使用默认付款账户、默认转账备注；
   5） 我的缴费记录、历史搜索记录等，大部分输入操作均在当前页执行，非必填项设置默认值减少用户输入操作；
   6） 应支持实时语音识别、语义智能纠偏等技术，提供无障碍支持；转账、生活缴费等常用功能需提供语音帮助模式，用户点击就可以语音播放相应的内容信息；
   7） 应提供多感官通道的信息传达和反馈方式，助力不同类型用户理解业务、

熟悉操作；

8）应支持语音搜索，帮助用户快速定位产品功能；

9）应提供字体“一键放大”功能；

10）除图形验证码（视障人群无法使用）外，需提供其他验证方式。

8.2 技术前瞻

移动金融客户端应用软件有以下技术创新方向：

a）智能客服：通过人工智能技术，实现实时应答，24 小时贴心服务，同时预设高频业务办理入口菜单，并提供高频问题自助答疑 QA 指引。

b）适老化安全性能力提升：通过亲情共管共控、风险交易监控等手段管控交易，防老年欺诈。

c）智能语音技术：通过语音搜索，为用户提供快速触达产品、功能等全量服务的搜索快捷入口。

d）智能消息推送：以“推送＋用户确认"，实现移动金融客户端消息推送功能。根据用户日常行为主动推送，用户可修改推送规则；理财到期前自动推送新产品预约；主推的权益或活动提醒和推送；在合适的时候，通过短信、微信以及客户端推送等多种形式推送给用户。

参考文献

[1] GB/T 25069—2010 信息安全技术术语
[2] GB/T 35273—2020 信息安全技术个人信息安全规范
[3] JR/T 0149—2016 中国金融移动支付支付标记化技术规范
[4] JR/T 0156—2017 移动终端支付可信环境技术规范
[5] JR/T 0171-2020 个人金融信息保护技术规范
[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 0068—2020 网上银行系统信息安全通用规范
[8] 中国人民银行. 中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号），2016-6-13
[9] 中国人民银行. 中国人民银行关于印发《中国人民银行金融消费者权益保护实施办法》的通知（银发〔2016〕314号），2016-12-14
[10] 中国人民银行. 中国人民银行办公厅关于加强条码支付安全管理的通知（银办发〔2017〕242号），2017-12-22