Q/GZYH

赣州银行股份有限公司企业标准

Q/GZYH 003-2023

代替 Q/300700 GZYH 003-2022

赣州银行移动金融客户端服务规范

2022-8-9 发布　　2022-8-9 实施

赣州银行股份有限公司　　发布

目录

1 范围

本标准明确规定了赣州银行向用户提供移动金融银行服务时的功能要求、安全要求、性能要求、服务质量和制度保障要求等内容。

本标准适用于赣州银行所属机构，通过移动互联网渠道，在移动设备向用户提供移动金融业务的服务。

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。凡是标注日期的引用文件，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。

中华人民共和国电子签名法

GB/T 32315-2015 银行业客户服务中心基本要求

JR/T 0068-2020 网上银行系统信息安全通用规范

JR/T 0118-2015 金融电子认证规范

GB/T 38556-2020 信息安全技术 动态口令密码应用技术规范

JR/T 0092-2019 移动金融客户端应用软件安全管理规范

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

3 术语与定义

下列术语和定义适用于本规范。

3.1 移动金融客户端

本规范所称的移动金融客户端（指“赣州银行”App，以下简称“App”）指通过移动通讯网络向客户提供的账户管理、转账汇款、手机支付、投资理财、定期存款、自助缴费等各类金融服务。

3.2 APP 客户

APP 客户是指签约使用移动金融客户端的客户。

3.3 敏感数据

敏感数据是指一旦泄露可能会对用户或机构造成损失的数据，包括但不限于：用户敏感数据（如用户口令、密钥等）、系统敏感数据、其他需要保密的敏感业务数据、关键性的操作指令，以及其他需要保密的数据等。

3.4 收集

获得个人金融信息的控制权的行为。

4 服务安全性

移动金融客户端的安全技术、安全管理、业务运作安全、信息保护等均应需符合JR/T00802《网上银行系统信息安全通用规范》、JR001-2012《金融行业信息系统信息安全等级保护实施指引》、T01562017《移动终付可信环境技术规范》、GBT2239-2019《信息安全技术网络安全等级保护基本要求》，部分规定具体转化如下：

4.1 安全技术要求

4.1.1 客户端安全

客户端从开发及使用的安全角度需满足以下基本要求：
（1）客户端程序应采用代码混淆和客户端加固等抗逆向分析措施，防范攻击者对客户端程序的调试、分析和篡改。
（2）客户端应使用企业级的证书对客户端进行签名发布，在程序运行时，对其真实性和完整性校验，发现客户端程序被慕改后，停止提供服务。
（3）重要信息（客户或用户敏感信息）不应在本地存储，如需存储，应保留最少的客户信息，经过加密处理，并限制数据存储量和保留时间，防止本地信息存储导致敏感信息泄露。
（4）应屏蔽客户端运行时日志输出、关闭客户端日志输出标志及函数。
（5）客户端权限设置应遵循最小授权原则只赋予客户端完成操作的必备权限和最少功能，防止权限过大，被恶意代码利用。
（6）应使用官方编译软件对客户端进行编译处理。
（7）客户端应对输入字符的合法性进行判别并过滤非法字符，防止注入等攻击。
（8）客户端应对服务端 SSL 证书的有效性进行校验，防止中间人攻击。
（9）客户端应对用户终端设备的指纹信息进行采集，并和用户建立一对一绑定、一对多绑定、多对一绑定或多对多的绑定关系。
（10）应对客户端款件进行合理配置，保证客户端软件的安全性。

4.1.2 服务端安全

（1）合理设计系统网络架构。应在互联网边界部署如防火墙、IDS/IPS、DDos 防护等访问控制、入侵防范相关安全防护能力的网络安全防护措施。
（2）服务器应部署在接入安全防护设备之后的逻辑隔离区域（如前置网络区域），通过互联网访问相关应用服务。
（3）客户端与服务端的通信传输使用 TLS 协议，保证传输数据的机密性和完整性。
（4）定期实施渗透测试，及时发现并修复系统存在的安全漏洞。

4.1.3 网络与通信安全

（1）接入本行内部网络的各类设备应通过本行指定的渠道访问互联网。业务网通过互联网接入区主动连接互联网应仅能访问指定第三方或限定特定端口进行访问控制。
（2）敏感数据在行外传输，应使用 TLS1.0 以上版本的传输协议，保证传输数据的机密性和完整性。
（3）应使用安全的数据提交方式，禁止在 URL 中传输明文的账号、密码、业务数据等敏感信息，应以表单方式提交。
（4）应采取有效措施在客户、用户及公司内部敏感数据在显示时，进行脱敏处理。

4.1.4 身份认证

（1）应该采取有效措施保障身份认证的安全性。
（2）使用安全的口令策略和登录失败错误处理策略，在身份认证时，防止账号口令暴力猜解。
（3）应采取有效措施防止登录重放等常见漏洞。
（4）应采取有效措施保护身份鉴别信息输入安全，传输安全和存储安全。
（5）支持生物特征（包括人脸识别、指纹）、短信动态码、图形密码等多重身份认证。

4.1.5 安全审计

（1）应具有覆盖到每个用户的日志记录功能。
（2）审计内容应包括重要的敏感操作，如用户账户登录信息、权限变更等。
（3）对于每一个事件，其审计记录应包括事件的日期和时间、IP 地址、访问者标识、事件类型、事件结果变更事项等内容。
（4）不应在日志中记录密码、支付敏感信息等重要数据。
（5）应对日志记录进行保护，确保日志不被他人非授权访问、修改或删除。

4.2 安全管理要求

4.2.1 安全管理机构

安全管理机构应满足以下要求：
（1）应设置移动金融客户端产品设计，系统研发、测试、集成、运行维护、管理，内部审计团队，业务、技术、审计等各相关人员应明确自身信息安全保障及风险管理职责，相关人员应详细了解本部门个人手机银行相关的职责设置、信息安全保障机制等基本情况。
（2）应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离。
（3）应加强机构内部及其与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，增强日常安全防护、突发事件处置、故障处理等方面的能力。

4.2.2 安全策略

安全策略应满足以下要求：
（1）应制订移动金融客户端系统使用的网络设备。主机设备、安全设备的配置和使用的安全策略。
（2）应做好移动金融客户端相关的新产品（业务）设计以及主要技术路线选择等关键规划的深入论证工作，关注产品及技术路线的合规性、相关业务及技术规则的一致性和延续性以及产品间、系统间的关联性、依赖性，平衡客户体验和安全性，通过增加关键控制机制等措施防范潜在重要安全隐患，避免产生潜在的信息安全风险。

4.2.3 管理制度

管理制度应满足以下要求：
（1）应建立贯穿移动金融客户端业务运作、系统需求分析、设计、编码、测试，集成、运行维护以及评估、应急处置等过程的相关安全管理制度。
（2）应指定或授权专门的部门、人员负责安全管理制度的制定、修订。
（3）安全管理制度应统一的格式，并通过 OA 发布审批，发布。
（4）应根据实际需要对管理制度的有效性及合理性进行审计、修订。

4.2.4 系统建设管理

系统建设应满足以下要求：
（1）根据系统建设、变更的等级测评、安全需求评估等的结果，确定安全管理策略、安全设计方案等相关文件。
（2）系统建设在需求、设计、开发、测试全生命期中，应符合系统建设过程安全管理办法，保证信息系统安全投产运行。
（3）应确保安全产品采购和使用符合国家的有关规定。
（4）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

4.2.5 系统运维管理

系统运维应满足以下要求：
（1）应对通信线路、主机、网络设备和应用的运行状况、网络流量、用户行为等进行监测和报警，建立监测指标，有效监测、预警个人手机银行安全事件（风险）。应及时采取控制措施，消除监测到的安全威胁。
（2）系统变更应做好风险评估、数据备份及应急预案，对风险较大的变逆，应做好变更后系统运行监控及跟踪工作。
（3）应根据系统数据的重要性和数据对系统运行的影响，制订系统数据的备份和恢复策略。

4.2.6 个人信息保护

（1）在收集、使用客户信息之前，应明示收集、使用信息的目的、方式和范围，公开其收集、使用规则，并取得客户的明示同意。
（2）客户端应用程序在采集客户个人信息前应对采集的用途和必要性进行提醒。对可能发生的信息泄露、损毁、丢失的情况，应明确提出将承担法律责任，并及时通知受影响的用户和采取补救措施。
（3）存储、传输个人生物识别等信息时，应采用技术措施对生物识别等信息进行保护，避免信息泄露，保护个人信息的机密性、完整性、可用性。
（4）在采集查看、修改个人信息时，应对用户 ID 等关键输入参数做安全校验，防止 SQL 注入、越权查看、修改他人信息。
（5）应向客户提供能够查看、更正、删除其个人信息，以及撤回授权同意，注销账户、投诉等方法。
（6）最小必要：只处理满足个人信息主体授权同意的目的所需要的最少个人信息类型和数量。目的达成后，应及时删除个人信息。

4.2.7 风险管理

移动金融客户端需接入交易监控平台，对交易数据进行实时监控及分析，根据风险高低产生预警信息，从而实现欺诈行为的监测、识别、预警和记录。

5 客户体验

5.1 客户端更新及使用

（1）APP 应具有易访问性，保证用户随时触达，包括但不限于官网入口、各大应用市场支持下载，且软件安装过程简单。
（2）APP 应具有可辨识性，功能分类清晰，确保用户能在首次接触时就了解该系统的主要功能，用于判断是否满足自己需求。

（3）APP 在不影响功能实现的前提下，要提升操作的便利性，减少操作步骤，方便用户的使用。

（4）APP 要通过产品设计，采用统一的交互、规范，统一的操作规则，避免用户可能会出现的操作失误。

5.2 基本安全措施

（1）安全键盘；
（2）登录安全提示；
（3）超时退出机制；
（1）防范登录操作重放攻击；
（2）防截屏提示；
（3）设备绑定；
（4）密码安全措施，输入密码等不得明文显示，多次输错密码处理机制；
（5）其他基本安全措施；
（6）安全检测：基本风险检测和程序/代码、用户数据、验证码等。

6 创新及前瞻性

6.1 服务创新性

创新服务的业务流程及风险控制应符合监管部门的要求。

6.2 适老化及无障碍化使用

APP 服务应提供简洁版本：UI 简洁界面、字体放大，简化操作流程。提升 APP 的兼容性与稳定性，满足用户视图、使用辅助等方面的特殊需求，降低老年客户群体以及信息障碍人群使用金融服务的门槛。

6.3 技术前瞻

6.3.1 生物识别

在仅采用人脸特征识别系统，错误拒绝率≦5%的情况下，企业标准文本要求错误接受率≦0.01%。应满足以下要求：

（1）交易不应单独只依赖生物识别做为唯一的身份认证方法；

（2）生物识别应当设置错误次数上限；

6.3.2 指纹识别

移动金融客户端指纹识别应满足以下要求：

（1）指纹识别不宜单独做为身份识别及认证的方法；

（2）指纹识别应当设置错误次数上限；

（3）当录入的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。

7 管理制度与企业标准宣传

7.1 系统突发事件管理

App 的应急响应机制应当遵循《赣州银行电子渠道业务连续性计划》。

7.2 宣传

（1）加强全行人员企业标准教育和风险提示，向员工详细解释本机构移动金融客户端应用企业标准；

（2）积极开展 App 业务功能宣传与培训，确保业务人员能全面熟知 App 的功能，熟悉 App 的操作，能向客户介绍 App 的功能及使用方法。

7.3 培训

应采用多种方式不定期组织相关人员参加 App 服务标准相关培训，确保相关人员具备必要的专业知识和能力，继而推进 App 业务快速发展。

7.4 监督

通过定期检查等方式监督标准落实情况，对未落实的方面，及时进行整改。