

Q/GZYH

赣州银行股份有限公司企业标准

Q/GZYH 001-2023

代替 Q/GZYH 001-2022

赣州银行网上银行服务规范

2023-8-31 发布

2023-9-1 实施

赣州银行股份有限公司

发布

目录

1 范围.....	3
2 规范性引用文件.....	3
3 术语与定义.....	3
4 服务安全性.....	5
5 客户服务.....	8
6 创新及前瞻性.....	9
7 管理制度与企业标准宣传.....	10

1 范围

本标准明确规定了赣州银行向用户提供网上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，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

3 术语与定义

下列术语和定义适用于本规范。

3.1 网上银行

本规范所称的网上银行指通过移动通讯网络向客户提供的账户管理、转账汇款、支付、投资理财、定期存款、自助缴费等各类金融服务。具体包括：个人网上银行、企业网上银行。

3.2 个人网上银行

个人网上银行（简称“个人网银”），是指赣州银行通过互联网向客户提供在线业务办理功能和服务的业务受理渠道。

3.3 企业网上银行

企业网上银行（简称“企业网银”），是指赣州银行通过网上银行向客户提供的包括查询、转账、对账、理财等金融服务的一整套体系。

3.4 个人网上银行

3.4.1 申请与开通

个人可持有效身份证件及我行借记卡通过赣州银行柜面、智能设备等方式，面对面向我行申请开通个人网上银行。客户办理业务申请时，应年满 16 周岁，应出具的有效身份证件包括：居民身份证、港澳居民居住证、台湾居民居住证、港澳居民来往内地通行证、台湾居民来往大陆通行证、外国人永久居留证（永久居留身份证）、外国护照。

对于申请理由不合理，开立业务与客户身份不相符，有明显理由怀疑客户开立电子银行存在倒卖或异常行为的，可拒绝办理。

3.4.2 关闭及注销

客户可通过柜面及赣州银行手机银行办理关闭网上银行，通过柜面办理手机银行办理个人电子银行解约（注销）。柜面解约可由他人代办，需持客户本人及代理人有效身份证件办理。

3.4.3 交易功能

个人网银为客户提供账户管理、转账汇款、理财、存款、生活缴费、电子社保卡、网点服务等功能。

3.5 企业网上银行

3.5.1 申请与开通

拥有在本行开立的单位结算账户，包括基本账户、一般结算账户、专用账户、临时账户等（有效期内）可至柜面申请签约开能企业网上银行。

客户填写《赣州银行单位综合业务服务申请表》，申请表内容不得涂改。提供企业账户开户证件（指营业执照、证明文书等企业证件/机构证明材料，下同）、企业法人身份证件、企业操作员身份证件的原件。非企业法人亲自办理的，还需出具《赣州银行人民币结算账户业务授权书》及企业经办人身份证件原件。

3.5.2 关闭及注销

客户至可至我行柜面办理企业网上银行注销。填写《赣州银行单位综合业务服务申请表》，提供企业法人身份证件原件。非企业法人亲自办理的，还需出具《赣州银行人民币结算账户业务授权书》及企业经办人身份证件原件，向签约机构申请办理解约。

3.5.3 交易功能

企业网银为客户提供账户管理、转账汇款、理财、存款、电子票据、银企对账等功能。

3.6 网上银行交易验证

本行为企业及个人网上银行客户提供短信验证码、人脸识别、设备绑定、UKEY 认证等交易验证方式。网上银行系统向客户颁发中国金融认证中心（简称 CFCA）的证书，客户通过企业及个人网上银行办理重要业务时，必须采用证书进行签名认证。

4 服务安全性

网上银行的安全技术、安全管理、业务运作安全、信息保护等均应符合 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，发现客户端程序被篡改后，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）应对客户端软件进行合理配置，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测。
- (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) 应设置网上银行产品设计，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) 应制订网上银行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) 应做好网上银行相关的新产品（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) 应建立贯穿网上银行业务运作、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，对风险较大的变更，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的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，修改个人信息等方法。

4.2.7 风险管理

网上银行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 客户服务

5.1 网上银行基础功能

个人版网上银行基础功能包括登录、注册、忘记密码、网点查询、无卡取款预约/撤销、账户管理、预留信息设置、公告、客服、意见反馈等。

企业版网上银行基础功能包括登录、转账、电子回单、账户查询、电子票据等。

5.2 身份认证

5.2.1 个人网银身份认证

本行为个人客户提供登录密码、U K E Y、图形验证、短信验证等交易验证方式。客户登录网上银行时，如密码输入错误达到一定次数时，会限制客户登录操作。需次日解锁或到柜面解锁。

5.2.2 企业网银身份认证

本行为企业客户提供登录密码、U K E Y 等交易验证方式。客户在进行动账时，需输入 U K E Y 密码进行认证。同时，根据企业操作员权限，对动账类交易进行相应审核操作，确保交易安全性。客户登录企业网上银行时，如密码输入错误达到一定次数时，将限制客户登录操作。

5.3 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。

5.4 客户服务质量

呼叫中心客户服务质量方面，须遵照 GB/T32125-2015《银行业客户服务中心基本要求》、GB/T32312-2015《银行业客户服务中心服务评价指标规范》和 T/CBA204-2019《远程银行客户服务与经营规范》严格执行。

5.4.1 服务路径

包括但不限于：

客户服务热线：0797-96296 和 4008496296；
微信公众服务号：赣州银行
在线客服入口：网上银行登录页面下方

5.4.2 服务时间

客户服务热线 7×24 小时；
微信公众服务号和在线客服：8：30-22：00

6 创新及前瞻性

6.1 服务创新性

- (1) 统一用户体系，实现一套账户密码登录手机银行 APP、网银；
- (2) 针对不同客群的差异服务需求，提供面向专属客群的差异化版本服务能力；

6.2 适老化及无障碍化使用

应提供简洁版本：UI 简洁界面、字体放大，简化操作流程。提升系统的兼容性与稳定性，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

本行网上银行系统应持续保持技术敏感性和技术前瞻性，积极稳妥引入行业先进技术手段，具体要求如下：

- a) 密码产品应实现全面国产化，应取得国家密码管理局商用密码产品型号证书。
- b) 关注并积极探索引入生物识别技术，同时不断提升相应的风险防范能力。
- c) 关注并逐步采用行业领先的底层技术架构，实现无感升级、灰度投产，提升客户使用体验。
- d) 应逐步探索使用大数据及人工智能技术，以帮助客户精准获取满足需求的产品和服务。

7 管理制度与企业标准宣传

7.1 系统突发事件管理

网上银行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网上银行应用企业标准；

（2）积极开展网上银行业务功能宣传与培训，确保业务人员能全面熟知网上银行的功能，熟悉网上银行的操作，能向客户介绍网上银行的功能及使用方法。

7.3 培训

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

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，及时整改。