ICS 03.060
A11

Q/131003L

廊坊市广阳舜丰村镇银行移动金融客户端服务企业标　　准

Q/131003L003—2024

廊坊市广阳舜丰村镇银行移动金融客户端服　务

Financial mobile application　Service of Lang Fang Guang Yang ShunFeng Rural Bank

2024 - 10 - 10 发布　　2024 - 10- 10 实施

广阳舜丰村镇银行　　发 布

目　　次

前　言

本标准根据JR/T0092-2019移动金融客户端应用软件安全管理规范起草制定。
本标准由廊坊市广阳舜丰村镇银行股份有限公司提出。
本标准起草单位：廊坊市广阳舜丰村镇银行股份有限公司。
本标准主要起草人：财务会计部
本标准为首次发布

引　　言

本标准内容涉及服务安全技术、操作风险和防范措施、实施保障三个方面，旨在明确移动金融客户端服务企业标准，增强移动金融客户端安全防范能力，促进移动金融客户端规范、健康发展。

廊坊市广阳舜丰村镇银行移动金融客户端服务企业标准

1 范围

本标准规定了移动金融客户端服务要求，明确了安全性和服务标准，确立了服务实施保障机制。
本标准适用于本行所有机构。

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 32315-2015 银行业客户服务中心基本要求
GB/T 35273-2020 信息安全技术 个人信息安全规范
JR/T 0171-2020 个人金融信息保护技术规范
JR/T 0092-2019移动金融客户端应用软件安全管理规范
JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引

3 术语与定义

下列术语和定义适用于 Q/131003L003—2020 的本标准（本部分）。

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。

3.2

电子回单 Electronic Reply
电子回单是为移动金融客户端客户提供的以电子化方式查询、打印和补打回单的功能。

3.3

交易过程 TRANSACTION
基于计算机传输商务信息，从而构成了通过全球网络进行方便通信的特定过程。交易通常是指在应用系统中一笔业务从开始请求状态转换到该笔业务结束状态所采用的一系列操作，一笔交易是通过对一组消息或软件包在交易平台上进行传递、转换和处理来完成的。

3.4

密钥 KEY

在进行加密处理时需要具备的一个可变因素，其目的在于使用同样的加密方法能够得到不同的加密结果。

3.5

个人数字证书 PDID

它是为某一个人或用户提供的证书，以帮助个人在网上进行安全地电子交易操作。个人身份的数字证书通常是安装在客户端的浏览器内，并通过安全的电子邮件进行交易操作。

3.6

支付密码 Payer Code，PC

它是一个由顾客设置的密码。它的哈希码（Hash码）H（Payer-Code）包含于支付信息中，以便顾客进行电子支付，商家存入货币后可向银行证实。银行将记录带有H（Payer-Code）的商家存款信息。如果顾客泄露了Payer-Code，银行能确定设置Payer-Code的顾客，并能进行准确无误的支付。

4 服务安全技术

4.1 物理安全

——物理安全风险：主要指系统周边环境和物理特性引起的设备和线路的不可用,而造成移动金融客户端的不可用。它是整个移动金融客户端安全的前提。如：设备被盗、被毁坏；链路老化或被有意或者无意的破坏；因电子辐射造成信息泄露；设备意外故障、停电；地震、火灾、水灾等自然灾害。

——针对上述风险，我行移动金融客户端必须制定如下策略：

- 所有移动金融客户端的关键设备都须放置在银行计算机机房内，机房的建设要完全按照国家标准，具备：门警、安保、防火、防水、恒温恒湿、防雷击、防电子辐射、持续稳定供电、防鼠咬等专用设施。
- 所有移动金融客户端关键设备都要有灾难备份，这些设备包括：移动金融客户端服务器和网络（安全）设备等。
- 所有移动金融客户端数据需要双备份制，这些数据包括：系统软件、数据库数据、访问日志等。考虑到移动金融客户端业务运行的连续性，必须设定每日定时，特别是增量备份，且备份媒体一式两份：一份放在本地机房的专用防火柜中，一份则放在异地备援中心的专用媒体柜中，确保重要数据的完整、安全与可靠。另外，为防止备份媒体的意外损坏或丢失，必须定期执行媒体测试与报废、设备保养，以及进行严格的媒体登记管理。
- 为跟踪设备的运行状况和操作记录，还必须执行严格的监控与登记制度，诸如：《机房运行日志》和《机房出入登记表》等。
- 制定《移动金融客户端灾难备份与恢复计划》，并定期测试演练，确保移动金融客户端系统安全、稳定地运行。

4.2 网络安全

4.2.1 数据传输风险分析

重要业务数据泄漏风险：由于在同级网络和上下级网络数据传输线路之间存在被窃听的威胁，同时局域网络内部也存在着内部攻击行为，其中包括：登录通行字和一些敏感信息，可能被侵袭者搭线窃取和篡改，造成泄密。如果没有专门的软件或硬件对数据进行控制，所有的网络通信都将不受限制地进行传输，任何一个对通信进行监测的人都可以对通信数据进行截取。这种形式的"攻击"是相对比较容易成功的，只要使用现在可以很容易得到的"包检测"软件即可。

重要数据被破坏风险：由于目前尚无绝对安全的数据库及个人终端安全保护措施，还不能抵御来自网络上的各种对数据库及个人终端的攻击。同时一旦不法分子针对网上传输数据做出伪造、删除、窃取、窜改等攻击，都将造成十分严重的影响和损失。存储数据对于系统来说极为重要，如果由于通信线路的质量原因或者人为的恶意篡改，都将导致难以想象的后果，这也是网络犯罪的最大特征。

针对上述风险，移动金融客户端必须采用重要数据加密技术（包括：MAC 校验技术）、网络防火墙技术、入侵检测与防护工具等，确保移动金融客户端传输信息的安全性、保密性和完整性。

4.2.2 网络边界风险分析

目前我行提供与互联网连接的移动金融客户端服务；并且，内部用户也有上网需求，因此现有的网络存在的安全风险主要有：

入侵者通过探测扫描软件获得网络及操作系统存在的安全漏洞，如：网络 IP 地址、应用操作系统的类型、开放哪些 TCP 端口号、系统保存用户名和口令等安全信息的关键文件等，并通过相应攻击程序对内网进行攻击。

入侵者通过网络监听等先进手段获得内部网用户的用户名、口令等信息，进而假冒内部合法身份进行非法登录，窃取内部网的重要信息。

入侵者通过发送大量数据包对内部网中重要服务器进行拒绝服务攻击，使得服务器超负荷工作以至拒绝服务甚至系统瘫痪。

我们知道网络安全隐患不仅来自外部网络，同样存在于内部网，而且来自内部的攻击更严重、更难防范。如果办公系统与业务系统没有采取相应安全措施，同样是内部网用户的个别员工可能访问到他本不该访问的信息。还可能通过可以访问的条件制造一些其它不安全因素（伪造、篡改数据等）。或者在别的用户关机后，盗用其 IP 进行非法操作，来隐瞒自己的身份。

针对上述风险，我行必须设立移动金融客户端的多层安全架构、严格的用户访问策略和用户管理制度，最大限度地防御非法访问。同时，还必须定期进行操作系统、数据库等的漏洞检测、补丁修订。设置入侵检测和防护系统，以及网络流量监测，通过定义“黑名单”，有效区分网络中的正常状态与异常

状态，及时发现与抵御内/外部的禁止性活动、越权访问、异常访问等事件。

4.2.3 网络设备的安全风险

由于移动金融客户端系统要使用较多的网络设备，如：交换机、路由器等。使得这些设备的自身安全性也会直接影响移动金融客户端系统和各种网络应用的正常运转。例如，路由设备存在路由信息泄漏，交换机和路由设备存在配置风险等。我们必须对网络设备中的一些特权用户口令进行加密；禁用某些不必要的默认配置等。

4.3 服务连续在线可信性

4.3.1 系统服务

移动金融客户端系统满足7*24小时不间断运行。

4.3.2 系统运维

系统运维由外包公司负责，我行及运维公司均配备7*24小时运维应急人员，负责一旦发生异常情况第一时间处理。

4.3.3 系统恢复时间（RTO）

系统主备双活，异地灾备，灾备系统切换在10分钟内完成。

4.3.4 系统可用率

网银系统可用率达不低于99.9%。

4.3.5 系统监控覆盖率

系统交易成功率、响应率可用率达到99%以上（监控粒度为交易级别）。

4.3.6 数据丢失时间

系统设有生产、灾备两套数据库，数据丢失时间RPO=0。

4.4 信息安全

移动金融客户端应用的安全需求并不能单独由网络安全措施来满足，由于其信息需要穿越多个网络

节点，并且通过未知的应用网关进行存储和转发，因此要求对信息进行“发送方到接受方”的保护。另外，银行还必须确保客户重要信息在其应用系统的安全保存。对此，我行移动金融客户端必须提供信息的鉴别服务、访问控制服务、机密性服务、数据完整性服务和不可否认性服务等。

4.5 系统安全

4.5.1 数据库安全

必须对重要数据加密存储；对默认的用户口令进行修改，并设置口令的复杂度、生存周期及登录失败次数；设定用户权限；确立审计和备份恢复策略等；定期进行数据库的漏洞检测、补丁修订和性能优化。

4.5.2 操作系统安全

禁止 Terminal Service、FTP 等危险服务；规定用户口令的有效期、长度、强度及登录失败次数；制定审计策略；禁止匿名用户访问；设定用户权限和备份恢复策略等；定期进行系统的漏洞检测、补丁修订。

4.6 应用安全

移动金融客户端应用系统的设计对于整个移动金融客户端来说也是至关重要的。它可能存在的安全风险是：移动金融客户端设备所在的 DMZ 区域和银行局域网络其它区域之间的非法访问；用户提交的业务信息被监听或修改；用户对成功提交的业务进行事后抵赖；外网非法用户对服务器的攻击；客服人员对移动金融客户端关键业务的处理不当等。对此，我行必须合理规划其移动金融客户端应用系统，并定期予以优化、升级以避免风险的发生。

4.7 技术选择

移动金融客户端业务的开展必须选择一种成熟的技术（包括：语音技术与网络安全技术等）解决方案来支撑，因此可能在技术选择上存在着技术选择失误的风险。这种风险既来自于选择的技术系统与用户终端软件的兼容性差导致的信息传输中断或速度降低的可能，也来自于选择了被技术变革所淘汰的技术方案，造成技术相对落后、网络过时的状况，导致巨大的技术和商业机会的损失。对于传统金融而言，技术选择失误，只是导致业务流程趋缓，业务处理成本上升，但对移动金融客户端系统而言，则可能失去全部的市场，甚至失去生存的基础。

我行在选择移动金融客户端的系统和网络安全集成商时，必须由事先成立移动金融客户端项目小组对各受托厂商，就信誉、经营状况、技术及客户评价等方面作审慎地市场调查及评估；与外包厂商讨论项目内容前，应视项目需要与外包厂商先签订保密合约；在订定外包合约时，须明确：委托业务范围与内容、委托期间及进度、交付结果及方式、提交相关开发文档清单、系统验收方法。知识产权的归属(含原始码、智能财产权)、转让的禁止说明、费用与支付方式、项目延误的罚则、其它事故所受损害的赔偿责任、资料安全与保密维护、问题发生及紧急事件的协调处理、契约的解除说明，以及保固与维护内

容等；项目小组应对外包厂商合作的项目履行监督之责，定期与外包人员开会检讨进度，并形成书面报告呈送分管领导；应根据银行的软件开发规范要求外包厂商提供相应的文档，并对外包厂商所提供之文档及内容作审核与确认，便于日后维护与管理。项目结束后，应定期或不定期评估外包厂商的经营情况、行业资质与产品更新，确保移动金融客户端系统在有效的技术支撑下，安全、稳定地运行。

我行还要及时跟踪信息（安全）技术的发展，特别要吸收国内外移动金融客户端的发展经验，并根据各 业务特色，通过培养更多移动金融客户端的业务与技术专业人才，设计与部署一整套性价比较高、适合长期稳定发展的移动金融客户端服务体系。

4.8 增强身份认证要求

客户登录移动金融客户端或登录后执行账户资金操作时，若身份认证连续失败超过5次，则锁定该客户在移动金融客户端的登录权限。

客户在通过移动金融客户端进行各项动账类操作时，系统会要求客户输入手机验证码来确认身份。

4.9 风险控制能力

建立风险交易监控平台，对短时间内单个客户的异常行为进行有效监控、适时阻断，并根据风险高低产生预警信息。

5 客户体验

5.1 服务功能

移动金融客户端应具备账户管理、支付结算、客户服务、交易复核等功能。

5.2 服务性能

5.2.1 易用性

移动金融客户端要满足以下要求：

易操作：交易菜单名称简单易懂；

易学性：交易操作简单、业务流程简洁，页面提示准确；

兼容性好：系统要兼容市面上常用的终端操作系统，并不断进行优化升级。

5.2.2 舒适性

移动金融客户端要满足以下要求：

统一页面风格、配色、字体大小、元素间距、常用控件样式及尺寸、页面布局等，保持产品设计风格一致；

页面提示友好、通俗易懂。

5.2.3 便捷性

移动金融客户端要满足以下要求：
交易菜单名称易查找、常用交易放在首页简洁实用显眼位置；
交易页面要素简单易懂，显示交易进度信息，页面信息提示准确；
页面交互流畅，交易结果提示准确；
提供交易结果查询功能，及时向客户反馈交易状态。

5.2.4 易访问性

移动金融客户端要满足以下要求：
登录方式简单，控件安装方便，兼容性强；
提供多种登录入口：网银助手、官方网站等；
官网提供网银助手及常用控件下载、常见问题的解决方案等；

5.3 客服代表行为规范

5.3.1 职业守则

客服代表职业守则主要包括：
诚实守信:诚实不欺，恪守信用，品行端正，树立诚信理念，坚持信誉至上；
遵纪守法:应以国家相关法律法规为行为准绳，严格遵守各项法律法规以及规章制度，认真学习法律知识，加强法律意识，自觉抵制违法违规行为；
勤业尽职:应热爱自己的职业、岗位，精益求精、尽心尽职、奉公无私、兢兢业业，以高度的热情和责任心投入本职工作；
专业胜任:应掌握相关业务知识，精通专业技能，根据社会发展、市场变化，在实践中不断学习新知识，钻研新技能，通过学习提高业务水平，适应工作发展的需要；
严格守密:应具备保密意识，保护商业秘密与客户隐私。严格遵守保密法规，自觉履行保密责任，做到不失密、不泄密。不得以任何个人目的或原因，泄露商业秘密和侵犯客户隐私；
宽容有礼:在工作中，会遇到各种各样的客户，在服务过程中，无论发生何种情况，都应时亥保持良好的观念和心态，保持宽以待人、谦虚诚实的态度，想客户之所想，急客户之所急，礼貌热情地为客户提供服务。

5.3.2 服务意识

客服代表服务意识要求主要包括:
应具有良好的心理素质和为客户服务的观念，保持积极的服务态度；
接通电话时客服代表应主动倾听，注意力集中;不随意打断客户，保持与客户之间的良好互动。不应表现出不耐烦、推托之辞等现象；
接通电话时客服代表应主动服务，有较强的语言表达技巧和沟通能力，思路清晰，恰当引导客；有效控制对话节奏，在客户对某些问题比较混淆时，能使用恰当语言总结性阐述客户问题，尽快切入正题，并能注意适当控制通话时间；

接通电话时客服代表应服务意识强，责任心强，积极主动的为客户解答问题，主动提供相关信息或帮助，包括为客户介绍金融产品及服务:指导客户使用电子渠道产品，引导客户使用办理相关业务的服务渠道、解决方法；帮助客户在线办理金融业务;了解客户需求，收集有益的客户建议，为改进服务和优化产品提供参考。

5.3.3 用语礼仪

客服代表用语规范主要包括:

客服代表应使用标准的开场白和结束语。正确使用服务敬语，耐心倾听，适时回应，主动感谢客户的帮助或配合，礼貌地结束电话；

客服代表应养成良好的通话习惯，保持恰当的语速和音量，通话时始终保持微笑、和蔼，吐字清晰、流畅自然；

服务用语应礼貌、规范，提倡讲普通话，实现语言无障碍服务。杜绝使用蔑视语、烦语、否定语。客服代表应在客户等待或客户等待后对客户表示款意:恰当的使用＂请、您…、谢谢对不起、请稍等”等礼貌用语；

客服代表不得使用服务禁语。严禁与客户争吵、顶撞、辱骂客户、主动或借故挂断客户电话等。

5.3.4 业务能力

客服代表业务能力要求主要包括:

客服代表应准确快速判断客户问题原因，了解客户实际需求:根据客户类别和业务种类，及时解决客户问题；

客服代表应熟练准确、回答完整，处理有效，正面回答，相关业务知识丰富，提示无遗漏并能提出适当建议，避免不必要持线；

客户服务代表应对于超出解答能力范围的问题，与客户重复确认，主动记录客户问题，及时处理客户意见，妥善处理客户投诉，并在必要时跟进。

6 实施保障

6.1 组织保障

本行移动金融客户端业务由财务会计部、风险合规部、营业室及各支行共同负责管理。

6.1.1 财务会计部职责

——负责组织制定移动金融客户端业务的各项规章制度。

——负责制定移动金融客户端发展规划、开展业务分析、统计、组织产品宣传和推广。

——负责移动金融客户端业务开办机构的资格审查。

——负责移动金融客户端内管系统参数配置、机构及柜员维护、角色设定及分配、银行公告发布等管理工作。

——负责组织系统内移动金融客户端业务培训。

——负责组织移动金融客户端业务需求提出、立项及产品研发。

——负责移动金融客户端业务系统升级改造测试工作。
——负责移动金融客户端网络维护工作的管理，确保网络畅通。
——负责向监管部门报送移动金融客户端相关业务报表等材料。

6.1.2 风险合规部职责

——负责移动金融客户端业务风险管控工作。
——负责向监管部门报送移动金融客户端相关业务报表等材料；负责与农信银沟通协调。
——负责对移动金融客户端业务需求进行论证，并提供科技支撑和服务。
——负责移动金融客户端应用软件项目、基础设施项目建设。
——负责协助金电公司托管中心保障移动金融客户端系统安全稳定运行。
——负责移动金融客户端系统安全管理工作。
——负责移动金融客户端安全技术方面培训。

6.1.3 营业室及各支行职责

——负责移动金融客户端业务宣传、营销工作。
——负责受理客户移动金融客户端业务申请，审核相关资料，办理注册、变更、注销等事项，负责客户资料、认证工具管理。
——负责对移动金融客户端落地业务进行审核。
——负责移动金融客户端全面风险管控工作。
——负责参与移动金融客户端资金汇划业务需求提出。
——负责移动金融客户端 USBKEY 等重要空白凭证管理、各支行重空使用监督工作。
——负责移动金融客户端产品价格管理。
——负责移动金融客户端内管系统机构管理员维护、角色设定及分配等管理工作。

6.2 岗位分工

6.2.1 移动金融客户端部岗位设置

——业务管理岗：设置专职岗位，负责组织制定移动金融客户端业务的各项规章制度；负责移动金融客户端业务开办机构的资格审查；负责移动金融客户端内管系统管理录入工作；负责组织系统内移动金融客户端业务培训；负责组织移动金融客户端业务需求提出、立项及产品研发；负责与农信银沟通协调工作；负责移动金融客户端业务指标制定、落实和考核。
——风险管理监控岗：设置专职岗位，负责移动金融客户端业务风险管控工作；负责监督检查移动金融客户端的运行和安全情况；负责对可疑交易、虚假交易的监控；定期组织安全评估，对移动金融客户端业务运营中出现的安全隐患及时提出控制措施；负责移动金融客户端内管系统管理授权工作；负责组织系统内移动金融客户端业务培训；负责参与移动金融客户端业务需求提出、立项及产品研发。
——业务测试岗：设置专职岗位，负责移动金融客户端日常业务及系统升级改造测试工作；负责参与移动金融客户端业务需求提出、立项及产品研发；负责拟定业务测试计划，按业务需求内容进行业务测试、联调测试。
——业务推广岗：负责制定移动金融客户端发展规划、开展业务分析、统计、组织产品宣传和推广。

负责督导全省移动金融客户端业务宣传、营销、新业务推广等工作。

——综合岗:负责移动金融客户端业务数据的收集、统计、汇总、分析工作；负责向监管部门报送移动金融客户端相关业务报表等材料；负责业务指标完成情况监测、考核；负责对移动金融客户端各项故障业务及可疑交易的通报工作；负责移动金融客户端综合管理工作。

6.2.2 信息科技部岗位设置

——业务开发岗：负责对移动金融客户端业务需求进行论证，提供科技支撑和服务；负责移动金融客户端应用软件项目建设。

——业务运维岗：负责协助金电公司托管中心保障移动金融客户端系统安全稳定运行;负责移动金融客户端系统安全管理工作；负责移动金融客户端基础设施项目建设；负责移动金融客户端安全技术方面的培训。

6.2.3 会计核算部岗位设置

——业务主管岗：负责辖内移动金融客户端业务全面工作。

——业务管理岗：设置专职岗位，负责贯彻落实本行制定的移动金融客户端各项规章制度；负责辖内移动金融客户端内管系统管理录入工作。

——风险管理岗：设置专职岗位，负责辖内移动金融客户端业务风险管控工作，对移动金融客户端业务运营中发现的安全隐患及时采取措施,自身无法解决的,须及时向移动金融客户端部汇报；负责辖内移动金融客户端管理系统授权工作。

——综合岗：负责移动金融客户端业务数据的收集、统计、汇总、分析工作；负责辖内业务指标完成情况监测、考核；负责向监管部门报送移动金融客户端相关业务报表等材料；负责移动金融客户端综合管理工作。

6.2.4 营业网点岗位设置

——业务推介岗：负责移动金融客户端业务宣传、营销工作。

——业务操作岗：负责受理、审核客户提交的移动金融客户端业务申请资料，办理客户移动金融客户端注册、变更、注销等事项，负责客户资料、移动金融客户端认证工具管理。

——业务授权岗：设置专职岗位，负责营业网点移动金融客户端业务风险管控工作，对移动金融客户端业务运营中发现的安全隐患及时采取措施，自身无法解决的，须及时向上级部门汇报；负责营业网点移动金融客户端管理系统授权工作。

6.3 管理制度

为确保本行移动金融客户端业务正常开展，规范和完善移动金融客户端业务管理，维护本行和客户的合法权益，本行先后制定了《广阳舜丰村镇银行移动金融客户端业务发展规划》、《广阳舜丰村镇银行移动金融客户端业务管理办法》、《广阳舜丰村镇银行移动金融客户端服务章程》、《广阳舜丰村镇银行移动金融客户端风险管理技术措施》、《广阳舜丰村镇银行移动金融客户端业务风险管理体系及规

章制度》、《广阳舜丰村镇银行移动金融客户端业务风险管理办法及策略》、《广阳舜丰村镇银行移动金融客户端业务运行应急计划和业务连续性计划》等。

6.4 企业标准宣传及实施机制

企业标准宣传:应建立企业标准宣传机制，借助自有和外部的宣传渠道，如官方网站、微信公众号、相关营销媒体及网点厅堂等，对企业标准进行宣传；

企业标准培训:应建立企业标准学习、培训机制，开发相应培训课程，全行进行学习；

企业标准实施监督机制:针对企业标准实施情况，应建立相应的监督机制，并定期组织检查定期公布检查结果，发现问题及时整改。