Q/BOCF

网　上　银　行　企　业　标　准

Q/BOCF 002—2021

中银富登村镇银行股份有限公司
网上银行服务企业管理标准

BOC Fullerton Community Bank Corporation

Internet banking system service enterprise management standard

2021－08－17 发布　　2021－08-17 实施

中 银 富 登 村 镇 银 行 股 份 有 限 公 司 发 布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中银富登村镇银行股份有限公司提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中银富登村镇银行股份有限公司，北京科蓝软件系统股份有限公司

本标准主要起草人：史炜捷、杨远红、林云、沈力克、马江华、孙旭强、周乙舜、刘琼、韦安升

网上银行服务

1 范围

本标准规定了个人网上银行应用软件开发的基本要求，从个人网上银行软件开发需要满足的运行条件出发，对个人网上银行软件开发提出了规范性要求。

本标准适用于提供金融产品和服务的金融机构，为个人网上银行应用软件的设计、开发、安全、运维及运营过程提供参考。

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。

JR/T 0092—2019 个人网上银行应用软件安全管理规范

JR/T 0171—2020 个人金融信息保护技术规范

3 术语与定义

下列术语和定义适用于本文件。

3.1

个人网上银行应用软件 personal internet banking 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。

3.2

金融机构 financial industry institutions

本标准中的金融机构是指由国家金融管理部门监督管理的持牌金融机构,以及涉及个人金融信息处理的相关机构。

3.3

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。

注1：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。

注2：[JR/T 0171--2020，定义3.2]

3.4

支付敏感信息　payment sensitive information

支付信息中涉及支付主体隐私和身份识别的重要信息。

注：包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

3.5

收集　collect

获得个人金融信息的控制权的行为。

注 1：收集行为包括由个人金融信息主体主动提供、通过与个人金融信息主体交互或记录个人金融信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人金融信息等行为。

注 2：如金融产品或服务提供者提供工具供个人金融信息主体使用，提供者不对个人金融信息进行访问的，则不属于本标准所称的收集。例如个人网上银行服务客户端应用软件在终端获取用户指纹等特征信息用于本地鉴权后，指纹特征信息不回传至提供者，则不属于用户指纹特征信息的收集行为。

注 3：[JR/T 0171--2020，定义 3.6]

3.6

转让　transfer of control

将个人金融信息控制权由一个控制者向另外一个控制者转移的过程。

注：[JR/T 0171--2020，定义 3.8]

3.7

共享　sharing

个人金融信息控制者向其他控制者提供个人金融信息。且双方分别对个人金融信息拥有独立控制权的过程。

注：[JR/T 0171--2020，定义 3.9]

3.8

明示同意　explicit consent

个人金融信息主体通过书面声明或主动作出肯定性动作，对其个人金融信息进行特定处理作出明确授权的行为。

注：[JR/T 0171--2020，定义3.22]

4　网上银行系统概述

4.1 系统标识

——名称：中银富登村镇银行网上银行系统；
——所属银行：中银富登村镇银行股份有限公司

4.2 系统描述

网上银行系统将传统的银行业务同互联网等资源和技术进行融合，将传统的柜台通过互联网、移动通信网络、其他开放性公众网络或专用网络向客户进行延伸，是商业银行等银行业金融机构在网络经济的环境下，开拓新业务、方便客户操作、改善服务质量、推动生产关系等变革的重要举措，提高了商业银行等银行业金融机构的社会效益和经济效益。网上银行系统主要包括通过PC、手机、平板电脑、智能电视、可穿戴设备等终端访问的网上银行系统，例如，手机银行、微信银行、直销银行、银企直联、小微企业银行等系统。网上银行系统涵盖个人网银系统和企业网银系统。

4.3 系统组成部分

a) 概述
网上银行系统主要由客户端、通信网络和服务器端组成，并可通过不同类型的通信网络连接到外部 系统，开展各类合作业务，其中服务器端包括网上银行访问子网、网上银行业务系统、中间隔离设备和 银行处理系统等。

b) 客户端
网上银行系统客户端主要包括客户端程序和客户端环境。客户端环境是指客户端程序所在的硬件终 端（目前主要包括 PC、手机、平板电脑、智能电视、可穿戴设备等终端，将来可能包括其他形式的终端） 及该终端上的操作系统、浏览器和其他程序所组成的整体运行环境。客户端环境通常不具备或不完全具 备专用金融交易设备的可信输入能力、可信输出能力、可信通讯能力、可信存储能力和可信计算能力， 因此，需要使用专用安全机制，并通过接受、减轻、规避及转移的策略来应对交易风险。金融机构应从 软硬件合法性验证、程序完整性保护、数据访问控制、数据输入安全、数据传输安全、数据存储安全以 及可信执行环境等方面保证客户端的安全性。

c) 通信网络
网上银行借助互联网、移动通信网络等技术向客户提供金融服务，易受到通讯层面的安全威胁，金 融机构应从通讯协议、安全认证、通信链路安全等层面，采取措施有效应对相关风险。

d) 服务器端
网上银行系统服务器端提供网上银行应用服务和核心业务处理功能，金融机构应充分利用物理环 境、通信网络、计算环境等领域的防护技术，在攻击者和受保护的资源间建立多道严密的安全防线。

e) 与外部系统连接
网上银行除直接向用户提供金融服务外，也可能与外部机构开展业务合作。在网上银行系统设计、 开发、部署和运营过程中，应充分考虑外部机构的系统可能存在的安全风险，并针对各类风险进行有效 防护。

f) 系统安全性描述
网上银行系统应根据应用系统、客户对象、数据敏感程度等划分安全域。通过对安全域的描述和界 定，可更好地对网上银行系统信息安全保障进行描述。 金融机构应采

取专用安全机制，包括数字证书、动态口令、短信验证码、生物特征等，保障网上银 行系统安全。

金融机构应按照其在交易中具备的可信通讯能力、可信输入能力、可信输出能力、可信存 储能力和可信计算能力五种能力的组合对安全机制进行分类管理，并制定与之适应的交易安全风险防范 策略。

金融机构在网上银行系统中应用云计算技术前，应结合网上银行系统的业务重要性和数据敏感性、 发生安全事件的危害程度等，充分评估应用云计算技术的科学性、安全性和可靠性，在确保系统业务连 续性、数据和资金安全的前提下，秉持安全优先、对用户负责的原则，充分评估可能存在的风险隐患， 谨慎选用与业务系统相适应的金融领域云计算部署模式。网上银行系统在采用云计算技术时应遵循 JR/T 0166—2018、JR/T 0167—2018、JR/T 0168—2018 等技术标准与行业主管部门的相关要求。

JR/T 0068—2020 网上银行系统在使用密码算法时应符合国家密码主管部门的要求，在支付敏感信息加密及传输、数 字证书签名及验签等环节宜支持并优先使用 SM 系列密码算法（GM/T 0002—2012、GM/T 0003—2012、GM/T 0004—2012）。

5 个人网上银行服务要求

5.1 管理功能要求

后台管理功能是个人网上银行服务系统的重要组成部分，用于各角色业务管理人员和IT系统维护人员的日常工作。

业务管理人员登录后台管理功能，通过操作图形化的工作界面，完成各类业务开展层面配置与维护。特定人员可以在后台管理功能与客户进行针对性的消息沟通。IT系统运维人员可以通过图形化的工作界面，实现对系统交易报文追溯、故障排查、性能监控的相关工作。

后台管理功能可以对各类人员和角色进行功能赋权。用户登陆网银后，根据人员的角色和权限，系统自动控制使用者可操作的功能以及可操作的具体金额。

在后台管理功能中实现业务功能开关和参数化配置，放到内存配置库中，快速响应业务变更，避免对后端数据库的读写压力。交易进行时，业务逻辑要动态进行后台管理功能配置的校验，避免个人网上银行服务获取的开关与参数值，与后台管理功能配置不同步造成交易失控。

5.2 基础配置功能

对板块配置、功能树配置、界面元素配置做到参数化，这三项是个人网上银行服务的基础工程。这三项功能有机结合，共同实现了在运营时快速响应业务需求，在线变更，减少版本发布，减少客户升级操作，增强用户体验的根本需求。要求个人网上银行服务客户端系统采用成熟开发架构，支持对业务变更的快速响应，减少客户升级更新操作。

5.3 板块配置

功能描述：业务部门管理人员在后台管理功能上动态配置、调整整个个人网上银行服务界面及其层级划分，即时生效。

5.4 功能树配置

功能描述：业务部门管理人员在后台管理功能上配置整个个人网上银行服务系统的功能树状结构，将具体的业务功能以特定展示形式放置到指定的板块区域内，展示形式包含如静态、上下及左右滚动展

示等，支持对业务功能的开启与停止设定，支持所有页面的跳转关系以及相关解说文字配置。用户操作后能够进入相应的业务功能受理界面。

5.5 界面元素配置

功能描述：业务部门管理人员在后台管理功能上进行配置、调整在个人网上银行服务界面上展示的所有界面元素、控件及其属性类型，如list、text、label、button、imag等，可对它们进行启用停用配置、文字属性和提示信息设置。

例如，客户在界面上进行外汇转账的撤单操作，客户提交前，管理人员在后台管理功能将撤单按钮置灰，并配置了停用原因。此时客户提交撤单，业务逻辑应该判断出后台管理功能已经更新了按钮为不可用，因此终止交易，并给配置好的提示信息。

对个人信息控制者的要求包括：

a) 在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容；

注：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。

b) 在向个人信息主体提供金融服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；

注：基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。

c) 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应：

1) 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项；
2) 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。

5.6 数据分析功能

建设面向互联网应用的数据统计分析模块，业务部门管理人员可完成个人网上银行服务电子渠道通用的客户各类资产查询 、统计、报表功能，并可生成EXCEL和PDF文件形式保存。优先以个人网上银行服务为应用目标，后期适配手机银行、微信银行等其他互联网渠道。要求项目交付成果对接CRM、个贷、信用卡等业务数据，以CRM系统数据维度为准。

5.7 数据统计与分析

个人网上银行服务通过客户行为埋点，统计用户的行为习惯，预测未来习惯趋势。能够对在个人网上银行服务上的浏览、设置、交易进行详尽的统计分析。能够对各银行产品业务受理和效果进行统计分析预测。通过设备信息、指纹等识别情况统计异常信息，出具个人网上银行服务异常事件分析报表。

日志分析：后台管理功能输入客户身份证号、卡号信息等查询到客户交易信息并区分失败和成功交易，对于查询日志的交易进行点击，弹出相应日志内容，日志内容包括请求报文、返回报文及明确错误信息。

5.8 客户标签与画像

功能描述：通过提取客户在个人网上银行服务操作的交易记录，对接 CRM 系统交易数据完成客户标签与画像。后期可服务于智能客服、电销平台、智能营销、智能风控等场景。根据客户资产，为客户建立星级体系，展示在客户个人网上银行服务上。

设定员工角色标签，提供分类信息推送服务

5.9 业务营销功能

实现营销接入、渠道接入，要求以客户行为为基础，根据客户在各电子渠道的所有旅程、节点，面向具体场景提供营销活动、广告宣传、信息推送、激励等综合营销服务的整体解决方案。要求业务部门管理人员在后台管理系统实现上述功能的动态配置。提供可视化配置，参数化配置，减少甚至杜绝二次开发。要求系统能够对所提供的推荐进行营销成果分析与统计，实现推荐营销成果的效益展示。

5.10 业务推荐

要求系统能够在用户操作前后某一特定时点，能够提供相关的业务功能推荐、银行产品推荐、资讯推荐、知识推荐以及相关的激励等。例如首页展示的智能提醒、功能推荐，理财等产品模块的智能推荐，转账类交易业务的常用转账人联想等。在相关场景下实现积分卡券的发放、使用，AR 扫红包奖励等。

可按照接入方、部门等维度配置业务营销信息。

5.11 广告系统

后台管理功能实现模板配置，在个人网上银行服务上展示后台管理功能配置的广告。业务人员可以登录后台管理功能，动态增加广告，随时配置广告所在板块ID、长宽高自适应、有效期、启用停用、图片（PNG、GIF）、视频（mp4、rmvb、avi等主流视频格式）、文字、链接。 广告配置后立即生效。广告可采用静态网页、动态链接、音频、视频等形式。

5.12 公告系统

后台管理功能可以向个人网上银行服务发布公告，展现在公告栏板块内。可以在个人网上银行服务通知栏以消息形式推送给客户，也可以在个人网上银行服务运行时动态弹窗展示。无论何种展示方式，客户最终都可以在公告栏内查看到公告历史。业务人员在后台管理功能进行公告配置，可以设定置顶，定时等功能。

5.13 营销统计

要求系统能够对所提供的推荐进行营销成果分析与统计，实现推荐营销成果的效益展示。

通过用户行为埋点，统计自身点击率，以及通过第三方接入的数据指标统计。

5.14 风险控制功能

智能风控模块通过对个人网上银行服务交易事件进行实时决策分析，配套风控策略体系，结合人脸识别、指纹识别等技术实现在每笔交易进行时实时调用风控最优方案。配合风控模型打造个人网上银行服务高效智能、安全可控的防火墙，最小化账户盗用、垃圾注册、暴力破解等风险。

a) 在安全控制层面，能够实现密码、数字证书、UKEY、人脸交易验证方式，结合具体业务场景，提供后台管理相应的开关配置。
b) 支持二类户身份认证时期的风险识别。
c) 提供手机设备自身安全检测功能。

d) 未来要求能够与安全管理部门进行对接，实现与原有系统的数据共享与分析，确保丰富现有系统的安全管理和风险控制功能。

5.15 流程体验功能

系统能够提供主动教学功能。例如在版本升级时提供新版本特性教学；在个人网上银行服务的特定场景与时机，也能够提供相应的动态教学功能，引导用户学习新的操作方法、介绍新的业务内容。要求后台管理功能实现教学环节、图片、文字、引导等内容配置。

a) 主动教学功能

系统能够提供主动教学功能。例如在版本升级时提供新版本特性教学；在个人网上银行服务的特定场景与时机，也能够提供相应的动态教学功能，引导用户学习新的操作方法、介绍新的业务内容。要求后台管理功能实现教学环节、图片、文字、引导等内容配置。

b) 被动教学功能

任意页面，客户停留 5 秒钟无响应时，弹出浮动的“业务说明”教学，用来向客户解释界面上的元素具体功能，操作流程、业务介绍。被动教学弹出时，客户可以忽略。要求后台管理功能可以配置被动教学。

c) 术语人性化

个人网上银行服务系统通过调用其他具体业务系统的功能实现客户服务，因此，在交易过程中，其他系统返回的提示信息、报错内容等文字并不能友好的被客户感知。因此，要求后台管理功能实现业务术语字典映射、过滤功能，能够对其他各类业务系统反馈的内容进行翻译，使得用户所见到的提示信息更加友好、易读、易理解。

d) 枚举字典配置

要求后台管理功能实现对各类枚举值的配置，更新后立即生效。例如对转账用途、分行名称、费用项等。

e) 其它个人网上银行服务配置

要求后台管理功能中动态配置可调用的第三方个人网上银行服务、微信小程序等应用。例如某部门建立了抖音号，在后台管理功能中做好配置后，在个人网上银行服务可以展现相关内容，点击后打开抖音指定内容。 微信小程序如乘车码、健康码等常用功能。

f) 智能知识库配置

为“语音/文字搜索”功能，在后台管理功能中配置知识库内容，实现智能推送。

g) 截屏功能

后台管理功能配置发生“截屏”操作后对应的功能。例如，当客户截屏后，可以弹出“召唤客服”选项。凡是弹出加密键盘时，不允许截屏。该功能需要与客服中心系统对接。

在后台管理功能平台上增加上传客户操作截图和操作视频的功能。由于后端看不到客户前端的操作，导致解决问题的时候排查面大，耗时长。

h) 消息服务功能

1) 统一消息服务

统一消息服务平台是服务于动账通知、验证码通知、活动通知等各种应用场景的综合性平台，可以为客户提供基于短信、微信、个人网上银行服务等互联网渠道的消息推送功能。要求后台管理功能实现对各类消息模板的可视化配置，能够对验证码类消息要求具有时效性配置。要求平台能够向指定客户群体发送设定格式的消息。

2) 消息推送

要求后台管理功能实现对个人网上银行服务的消息推送机制，并可以制定消息的种类与模板。业务管理人员可以在后台管理功能向所有或特定群体客户发送消息通知，消息展

示在手机通知栏内以及个人网上银行服务的“我的消息”栏目下。要求在各业务功能界面均提供快捷的消息入口和提示符。

3) 消息会话

实现银行各角色人员依据自身职能与客户聊天窗口形式图文消息收发需求。在窗口内可以向客户发送银行产品、业务功能链接、营销活动消息等功能。要求系统可以建立并维护不同角色的银行业务人员，每一角色人员可操作的功能与该岗位职能相关。要求能够合适的在各业务功能界面均提供快捷的消息入口和提示符。

以理财经理为例，登陆后台管理功能进入聊天页面，可以与特定客户进行图文消息沟通，推送特定理财产品购买入口。该理财经理可以看到当前会话客户的CRM信息，例如年龄、性别、职业、名下银行卡、最近交易、理财产品、信贷产品等详细情况，具体以 CRM 系统功能为准。客户经理等银行角色人员可以登录个人网上银行服务或相应的 web 端，展现与之相对应的功能布局，方便与客户继续沟通。

沟通记录永久保存，客户可以在个人网上银行服务中随时查看消息历史。本“消息会话”功能要与客服中心系统对接，实现坐席客服人员与个人网上银行服务客户的在线沟通。

人工客服服务时间满足 7×24 小时

i) 法律文书配置

1) 隐私政策与授权

在后台管理功能提供隐私政策文件的维护功能。可以编辑某一个版本，设置某一个版本为当前生效版本。服务端保存为HTML文件，便于前端读取。金融移动客户端用户只能看到当前生效版本。 一旦服务端当前生效版本更新，金融移动客户端弹出提示，用户必须勾选“同意并已读最新版本”，才能继续使用金融移动客户端。用户可以在任意状态下（无论是否登陆）都可以阅读最新版本的隐私政策。

在展现隐私政策文件的同时，提供对手机软硬件的相关授权，包含金融移动客户端系统使用到的所有权限。

2) 产品协议与说明书

业务人员在后台管理功能上配置各业务条线产品服务协议、产品说明书，实现对其内容维护、本管理、启用和停用。金融移动客户端随时可以获取最新版本展示给客户。要求以HTML或PDF形式配置到后台管理功能中，金融移动客户端可以在应用内打开HTML，也可以下载PDF文件到手机本地。

j) 服务咨询

1) 客户意见反馈

客户在金融移动客户端中输入文字、上传 5 张以内图片，向银行反馈意见。后台管理功能可以根据客户信息和意见类型查看这些信息。管理人员可以以消息、弹窗形式回复客户处置结果。

2) BBS 系统

后台管理功能可查看、回复、转发、删除、点赞客户在BBS上留言。在后台管理功能中，管理人员可以打开与关闭BBS系统。

3) 调查系统

后台管理功能可以配置调查问卷，金融移动客户端端以公告或弹窗形式展现调查问卷。

后台管理功能提供对调查结果的统计分析功能。

k) 个人网上银行服务版本控制

1) 版本的配置

安卓苹果版本号、启用状态（启用、停用）、升级提示信息、强制与建议更新，实现对不同版本的控制。

版本白名单：生产环境对某版本实现白名单登录功能，满足正式上线前的内测需求。

版本黑名单：对部分客户实现黑名单功能，在名单内的客户不得登录任意版本或某一版本。

2) 解除设备绑定

要求后台管理功能实现对指定的客户取消设备绑定功能，有利于特殊情况下服务客户需求。可以再度开启对该客户的设备绑定。

3) 插件化开发模式

要求对个人网上银行服务业务功能树中的功能，按照业务类型进行划分，实现插件化开发，有利于减少个人网上银行服务客户端安装包体积，有利于业务功能的动态发布管理及维护。用户可以动态选择安装部分插件。例如基金模块是插件，用户动态安装到本地后可以使用基金功能。再如，某营销活动开启了一个游戏场景，该游戏可以动态安装到本地。

1) 运维可视化

为提高系统运维人员的排障工作效率，监控系统运行状态，要求后台管理功能实现接口报文配置与跟踪功能。

1) 交易报文跟踪

为了提高运维人员追查交易报文的便利性，提高处理速度，降低工作压力，在当前统一接入平台后台管理功能上提供客户在个人网上银行服务操作行为记录查询以及个人网上银行服务报文跟踪功能。

要求系统能够对用户的交易进行报文跟踪，具体需求如下：

- 根据客户操作时序，按照个人网上银行服务系统与 ESB 系统交易过程：个人网上银行服务发送与接受的报文<------>个人网上银行服务服务端发送与接受的报文<------>统一接入平台发送与接受的报文<------>ESB 发送与接受的报文。
- 实现交易过程报文的全纪录与保存。
- 不包含其他具体业务系统调用的报文，只截止到 ESB 出入报文既可。

根据交易时序关系展现往来报文关系图。每一个环节都要给出相应的报文内容（请求报文、响应报文）。为了不影响业务交易的实时性，本功能数据库建立在单独的实例上，与业务交易数据库分离。库中内容保存 48 个小时（后台管理功能配置），自动清空。保留原有 log 文件形式的日志记录。

2) 客户行为追溯

要求系统能够全方位记录用户在个人网上银行服务上的所有行为与操作时间，包括但不限于浏览、点击、输入、滑动等操作。要求能够按照客户的操作时序关系，通过图形化、列表化的方式，重现并追溯用户的所有操作过程。

对于非正常情况，例如闪退、404、个人网上银行服务死机等情况，要将这些非正常情况的详细信息推送给后台管理功能并进行分析，有利与运维环节排查故障以及对个人网上银行服务端体验方面的优化。

3) 日常运维高效

为技术人员增加版本状态配置，简化版本部署流程，个人网上银行服务客户端操作痕迹报文可全流程追踪，日志便捷分析等功能。

5.16 个人网上银行服务客户端基础功能要求

a) 启动页

从现在节点起，体现了个人网上银行服务功能结果和要求。这个结构是可以在后台管理功能上配置的。

个人网上银行服务客户端是个人网上银行服务系统的重要组成部分，用于向客户提供银行各类服务，同时也是收集客户各类信息的入口。要求本项目交付成果，能够平迁当前个人网上银行服务功能不丢失，针对本项目要求提供增量功能。

启动页是个人网上银行服务给予客户重要的第一印象，也是个人网上银行服务最重要的黄金页面之一，所以个人网上银行服务启动页要做到以下两点：一是传播个人网上银行服务“一机在手、生活无忧”的定位，展现品牌形象，二是运营活动、广告推广。

b) 功能说明

用户首次下载个人网上银行服务时，首先显示 logo 页，然后采用滑动页的方式展示新版个人网上银行服务功能性，滑到点击“即刻体验”进入个人网上银行服务，弹出隐私政策，用户点击确认后，开始登录。

启动页加载完之后机内广告页面，广告页根据的活动、用户的生日、不同的节日显示不同的页面，显示时间在五秒以内。

日常无下载更新时，启动页为 logo 页，显示时间为两秒，有下载更新时，启动页也为 logo 页，屏幕中间有圆圈，更新时间最好不要超过五秒。

c) 首次使用教学

客户在个人网上银行服务更新后首次登录给出新功能首次使用教学，凸显更新后的本版个人网上银行服务主要特性。图示本次更新的内容和功能变动后的位置。每个页面中的说明内容尽可能不超过三项。

d) 登录功能

客户下载个人网上银行服务后，可登录个人网上银行服务进行相关操作。

登录按钮位于首页首行最左侧或者最右侧。点击后进入登录页面。如果客户不点登录钮，仍然可以浏览四个主栏目中不要求登录的内容。客户可以有多种登录方式，默认是二维码扫码登录，客户已开通其他登录方式都是有效的。

密码登录方式需要在开通时设定，二维码登录等方式在开通手机银行登录，打开手机银行，通过二维码扫码授权，登录个人网上银行服务客户端

登录页面展示：登录方式、自助注册、忘记密码。实现客户登录个人网上银行服务客户端的目的。

登录个人网上银行服务客户端 5 分钟内没有任何操作，自动退出登录状态。

登录方式——密码登录：采用登陆号+登录密码验证方式；密码键盘采用字母正序、数字乱序。

登录方式——手势登录：客户登录个人网上银行服务客户端后，在安全设置中可设置收拾登陆或修改手势登录。

登录方式——指纹/面容登录：客户登录个人网上银行服务客户端后，在安全设置中设置指纹/面容登录个人网上银行服务客户端。

自助注册：未开通个人网上银行服务客户端客户提供个人网上银行服务客户端号、短信验证码、姓名、绑定银行卡、OCR 身份认证。客户绑定他行卡时，可以生成二类账户。

忘记密码：客户忘记个人网上银行服务客户端登录密码时，可以通过此功能找回密码并登录个人网上银行服务客户端。手势、指纹/面容等方式忘记不能通过此交易找回。

e) 退出功能

退出个人网上银行服务。

登录后“我的”项下显示安全退出功能菜单，无登录时不显示退出登录菜单。

登录后，首页右上端显示“退出”标志。

客户点击“首页”退出或“我的”安全退出后，关闭个人网上银行服务。

客户在个人网上银行服务无任何操作 5 分钟，个人网上银行服务自动退出，提示客户“长时间未操作已退出，请重新登录”。

客户在操作个人网上银行服务时，同时进入电脑其他程序时，系统提示客户“个人网上银行服务已转入后台操作，请注意防范风险”。5 分钟内客户未返回个人网上银行服务，则提示客户“长时间未操作已退出，请重新登录”。

f) 公告、广告

显示后台管理功能公告、广告系统发布的信息。

展示 Banner 横幅、插屏、首页启动页、下拉刷新、视频等多位置、多形式广告、公告，相关位置可由后台管理功能统一设置。客户如果关闭广告推送等功能，相应广告不再为该客户展示。

客户在点击相关广告或公告位可以查看相关产品、信息详情或跳转至相关业务界面。

公告广告具有顺序可调，有效期可设等管理功能。

g) 资产总览

从 CRM 系统获取数据，显示客户所有资产的分布图。要求饼图，显示客户在的总资产情况（本行所有卡折），主要分为资产类（存款和理财）、贷款类（信用卡和贷款），并显示收支明细柱状图。

从积分系统获取客户已兑换或获得的红包、卡券或积分，在个人网上银行服务端提示客户，到积分商城中使用。通过个人网上银行服务增加个人综合积分功能，方便客户查询、兑换。个人综合积分是指使用制定金融产品所产生的积分，其中消费积分是指持有信用卡、借记卡消费可获得相应的积分回馈，有效期最长五年，当年累计积分将于第五年 12 月 30 日到期，当年记录为第一年。特定积分是指不定期开展的积分营销活动，针对满足条件的客户赠送相应积分回馈，具体规则及赠送的特定积分有效期以营销活动发布为准。个人网上银行服务支持个人综合积分的查询及在积分商城中的积分兑换功能。本需求仅对查询功能进行描述。通过新增个人网上银行服务个人综合积分查询界面客户可直接查询到有效期内的积分总额、本年到期积分、积分明细。

h) 账户管理

展示客户绑定的本他行借记卡、信用卡，以图片显示。后台管理功能中提供多家银行卡图样。用户可以便捷的查看每张银行卡的消费记录，可以快捷的用该卡还款、消费。增加按钮“同步到微信银行”，可以将该银行卡绑定到微信银行，同时提供删除功能。同步后，在微信中推送成功消息。重构当前界面设计和操作流程，提高客户体验，增加新卡的功能要突出。

1) 本他行卡图

显示绑定的一二类账户。点出卡图片，显示全卡号信息、开户行信息、开户时间、已签约业务种类、积分、银行卡的特征（比如钻石卡，白金卡、收费政策和权益，以及该卡可以参加的活动）复制卡号，并分别提供如下功能：

- 本行一类卡提供查询（可查余额、明细）、锁定（客户一时找不到卡时，可以锁定/解锁）、挂失、解绑等多项功能。
- 本行二类卡提供查询明细、转入转出、销户、修改交易密码等多项功能。

2) 未绑定本行卡折

提示客户在开立尚未绑定个人网上银行服务的卡折，提供绑定快捷操作，方便激活睡眠卡。

3) Ⅱ类户管理

主要有Ⅱ类户开户、密码忘记、绑定卡修改、销户等功能。

开户：卡号（本行Ⅰ类卡卡号）回显客户绑定的个人网上银行服务Ⅰ类卡卡号，卡号（非本Ⅰ类卡卡号行），则需要通过第三方渠道（如银联）进行验证。

i) 转账汇款

提供账号转账、手机号转账、语音转帐、一对多转账、好友转账等多种转账方式。提供转账好友名单。转账成功后，可提示客户手动添加到转账好友名单中，可生成电子回单，显示对手方明细，可保存可分享。提供功能联想，如查询余额、查询明细等功能。转账失败也要有提示，并可保存图片。

从转账好友名单中，可以进入转账功能。可以选择转账方式、认证方式。

银行账号转账：实现银行卡号之间的资金转账，包括行内转账和跨行转账。

手机号转账：输入对方手机号码的方式，实现卡卡转账业务，记忆方便、操作简单。下设签约、修改、查询、设置默认账户、解约等子功能。客户可以搜索其通讯录中，已开通手机号转账的朋友，方便使用手机号转账功能。

一对多转账：同一转账金额通过同一指定汇款人账户一次性转账到多个收款人账号。

好友转账：本功能通过好友名册，实现便捷转账。好友指曾经和客户发生过转账记录的联系人，包括转出和转入的联系人，同时好友列表支持增删维护。摒弃原有的收款人模式操作过程，提供新颖的面向社交的好友概念，好友名下具有本行他行银行卡，可以与好友进行图文消息发送。提供红包功能，使转账体验社交化。

预约转账：客户根据需要，预约转账日期，不冻结账户。在预约日发起转账时若客户账户余额不足，提示并发送信息给客户，账户余额不足，预约转账失败。

转账撤销：对转账方式为非实时转账业务，在发送前的时效内，客户可以提出撤销申请，撤销成功后资金回到原转出账户。

j) 交易查询

按交易时间、类型、渠道等方式，提供分类查询功能。可截屏保存图片或分享。汇入款项可以显示对方户名、账号、汇款银行等信息。查询结果中除了从核心返回的交易明细之外，还要包含预约、已完成、失败等所有状态的交易记录。

对于预约状态的记录，给出执行倒计时信息。给出立即执行按钮，用户点击后，立即转账，该操作结果仍要记录交易明细。同时本条信息标记为“已执行”。给出撤销按钮，取消本次转账，该操作结果仍要记录交易明细。同时本条信息标记为“已撤销”。最好提供撤销客户在 ATM 上的延迟转账操作。

交易时间：按照今日、近三天、一周、一个月、三个月、“自定义时间段”来查询。对于时间段过长的，给出“只支持 xxx 时间段的查询”。

交易类型：按照核心系统及网联、银联系统等第三方通道中的交易类型的交易明细，展示工资、商户消费、机票消费、话费消费等。具体类型划分以各系统提供的细分功能为准。用户点击相关类型按钮后，展现该交易类型下的所有交易记录。

交易渠道：按照核心系统及网联、银联等第三方支付公司的交易明细，要求界面提供网银、手机、银行柜台、支付宝、微信、银联等主流支付图标，用户点击图标后，展现该交易渠道下的所有交易记录。

交易金额：按照客户全部交易，要求界面提供小于 1 百、1 百-1 千、1 千-5 千、5 千-1 万、1 万-5 万、5 万-2 万、大于 20 万、自定义最小金额-最大金额区间查询功能，用户点击相应按钮或输入相应区间金额后，展现该交易金额区间下的所有交易记录。

收付款类型：按照客户全部交易，要求界面提供收款、付款查询功能。用户点击相应按钮，展现该交易收付款类型下的所有交易记录。

交易对手姓名：按照客户全部交易，要求界面提供收付款人名称查询功能，客户输入相应名称展现与该交易对手下的所有交易记录。

k) 资金归集

资金归集业务是指，在他行开立的银行卡，可以在本个人网上银行服务上设定自动转款日，或者手动操作，将指定金额的款项转入借记卡。

l) 周边网点

个人网上银行服务端可以展示和搜索网点和 ATM。优先展示与客户最近的网点或 ATM，调用地图可指示步行、公交车、自驾路线。能够展现该网点特色业务介绍、营业时间、理财经理电话、网点负责人电话，显示网点状态、业务内容和网点营休时间。

此功能需要与后台管理功能配合实现。业务管理人员登录后台管理功能，录入网点和机具的各类信息，展示在个人网上银行服务：网点名称，负责人及联系电话，理财经理及联系电话，百度地图坐标，特色服务介绍，营业时间，网点人性化设备情况。

建议为分行业务人员提供自行录入接口。

客户在网点列表中选择一家网点后，显示网点信息，以翻书方式查看。

无卡取款：下设申请、查询、撤销等功能。取现单笔、累计限额按照 ATM 规定执行，每天不限次数。

ATM 转账撤销：客户在 ATM 上做了预约转帐，可以在手机上查看并撤销。

ATM 扫码取现：配合支持此模块功能的自助机具提供扫码取现功能。

m) 收支帐本

客户通过银行账户系统、网联、银联等主要渠道完成的支付、收益、收款，均可记入收支账本，客户也可以自行记账。客户可以在账本中进行收支分类查询。提供本月账单、与上月账单对比，以折线图显示。提供年度账单。账单可下载、导出功能。

n) 智能推荐

根据客户使用或浏览个人网上银行服务产品偏好数据，以文字、图片、音视频提供新品推介，客户可以直接点击查看该业务产品。

o) 常用转账

个人网上银行服务客户端列出最近四笔客户通过个人网上银行服务发起的各类转账业务。

p) 常用缴费

个人网上银行服务客户端列出客户四笔近期缴费业务。用户点击后用原来的方式缴费，默认带出上次银行卡号和金额，客户验证支付就可以立即缴费，也可自行填写。

6 网银兼容性

个人网上银行应需兼容适配Android 5.0以上版本、IOS 11以上版本,在这些设备和系统版本升级过程中，需保证个人网上银行同步升级适配；

个人网上银行针对市场占有率超过5%的设备，确保UI界面的展示效果，没有错位、没有重叠，没有展示不全等展示问题；

个人网上银行需提供密码认证，短信认证等认证手段，可以提供刷脸认证、数字证书认证、声音认证，指纹认证等附加验证手段；

个人网上银行可以提供微信登陆或者支付宝登陆,第一次微信登陆或者支付宝登陆需要验证身份信息；

个人网上银行至少应兼容WIFI和3G网络以上信号；

个人网上银行应适配主流设备品牌和机型，包括定制版设备。

个人网上银行兼容IE和EDGE浏览器

6.1 网银的性能要求

a) 应用闪退率:Android 保持在 5/万以下，IOS 保持在 10/万以下。
b) 冷启动时间: Android 保持在 4s 以下，IOS 保持在 3s 以下。
c) 电量异常率： Android 保持在 0.001%以下，IOS 保持在 0.005%以下(电量异常定义:比如单位时间内的电量消耗超过阈值的数量比率,分子为当前异常数量、分母为当前所有的电量监控数据)。
d) 卡顿情况：Android 保持在 0.6%以下，IOS 保持在 0.8%以下(卡顿定义：主线程出现长时间卡顿 2.5S 以上的比例，分子为当前卡顿数量,分母为当且界面 PV 数量、分子比分母得到卡率数值说明用户操作界面出现卡顿的异常率)。
e) 流量异常情况：Android 保持在 0.006%以下，IOS 保持在 0.017%以下。(定义：流量异常（比如总流量超过阈值、重复请求等）的数量占比，分子为当日异常数量，分母为当日所有的流量监控数据)。
f) 消息推送：在线到达率 98%以上,离线到达率 60%以上。
g) H5 容器适配国内大多数机型，闪退率要求为：安卓低于 0.01%， IOS 低于 0.04%。
h) 网上银行系统服务时间是否满足 7×24 小时不间断运行，配备 7×24 小时运维应急人员
i) 网银系统可用率保持在 99.6%以上。
j) 数据丢失时间（RPO）应低于 3ms。
k) 系统恢复时间（RTO）应低于 30 分钟。
l) 可用性监控覆盖率不应低于 99%。

6.2 安全性要求

个人网上银行软件开发安全性要满足《中国金融移动支付客户端技术规范》（JR/T 0092）、《中国金融移动支付远程支付应用规范》（JR/T 0093）、《中国金融移动支付应用安全规范》（JR/T 0095）、《中国金融移动支付支付标记化技术规范》（JR/T 0149）、《移动终端支付可信环境技术规范》（JR/T 0156）、《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071），安全要求应包括但不限于以下点：

个人网上银行服务应用安全

a) 客户端软件加固

客户端打包发布前必须采取代码混淆、防反编译和防二次打包处理等安全加固措施。

b) 防范敏感信息泄露

在系统上线前，应删除个人网上银行服务目录下所有测试脚本、程序。如果在生产服务器上保留部分与个人网上银行服务应用程序无关的文件，应为其创建单独的目录，使其与个人网上银行服务应用程序隔离，并对此目录进行严格的访问控制。禁止在个人网上银行服务应用程序错误提示中包含详细信息，不向客户显示调试信息。禁止在个人网上银行服务应用服务

器端保存客户敏感信息。应对系统个人网上银行服务服务器设置严格的目录访问权限，防止未授权访问。禁止目录列表浏览，防止站点重要数据被未授权下载。

c) 防范 SQL 注入攻击

系统个人网上银行服务服务器应用程序应对客户提交的所有表单、参数进行有效的合法性判断和非法字符过滤，防止攻击者恶意构造 SQL 语句实施注入攻击。禁止仅在客户端以脚本形式对客户的输入进行合法性判断和参数字符过滤。数据库应尽量使用存储过程或参数化查询，并严格定义数据库用户的角色和权限

d) 防范跨站脚本攻击

应通过严格限制客户端可提交的数据类型以及对提交的数据进行有效性检查等有效措施防止跨站脚本注入。应对个人网上银行服务提供的链接和内容进行控制，定期检查外部链接和引用内容的安全性。

e) 客户端应用软件完整性要求

应对客户端应用软件进行签名，标识客户端应用软件的来源和发布者，保证客户下载的客户端应用软件来源于所信任的机构

客户端应用软件启动和更新时，应进行真实性和完整性校验，防范客户端应用软件被篡改。

应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力。

应能监测并向后台系统反馈个人网上银行服务客户端支付环境安全状况，并将此作为风控策略的依据。

6.3 通讯安全

a) 应在客户端与服务器之间建立安全的信息传输通道，通过公开网络进行数据传输时应通过密钥、证书等密码技术手段进行双向认证，如使用安全套接字层或传输层安全（SSL/TLS）、互联网协议安全（IPSec）等协议。

b) 在满足法律、管理规定的前提下，客户端应保留最少的客户信息，并限制数据存储量和保留时间。

c) 客户端在使用支付敏感信息后，应及时清除。

d) 应支持页面回退清除密钥、密码等敏感信息的机制。

6.4 访问控制

a) 应建立安全的访问控制机制，防止用户访问无权访问的功能或资源，例如越权访问他人账号的信息、在低级别的认证方式下访问高级别认证方式才能访问的功能等。

b) 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

c) 应建立完善的交易验证机制，每次处理的客户信息均以服务器端数据为准，并对客户请求指令的逻辑顺序进行合理控制。

6.5 交易安全基本要求

应按照《中国金融移动支付支付标记化技术规范》（JR/T 0149-2016）的相关要求，对银行卡卡号、卡片验证码、支付账户等信息进行脱敏，支持基于支付标记化技术的交易处理，采取技术手段从源头控制信息泄露和欺诈交易风险。

6.6 安全审计

a) 应具有保存和显示客户历史登录信息（例如，时间、IP 地址、MAC 地址等）的功能，支持客户查询登录（包括成功登录和失败登录）、交易等历史操作。

b) 应具有详细的交易流水查询功能，包括但不限于日期、时间、交易卡号、交易金额和资金余额等信息。
c) 审计功能应覆盖所有数据的管理操作，包括用户开通、证书发放、密码修改、冻结解冻、权限变更等操作，应对用户开通、专用安全设备更换、重要信息变更、冻结解冻等重要操作进行稽核。
d) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，并定期备份审计记录。

6.7 密码输入安全

登录密码和交易密码输入必须使用安全密码输入控件，密码输入控件要求使用国密算法；交易密码加密算法使用国密算法；客户端缓存数据要求使用国密算法；动态口令要求由支持国密算法的服务器产生；其它如涉及到加密的建议尽量使用国密算法。

6.8 认证方式

a) 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、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) 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，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。
   2) 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。
   4) 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，客户端源文件中不应包含图形验证码文本内容。
   5) 图形验证码不得作为独立的身份验证要素。增强要求。
   6) 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。
   7) 在用户身份认证后，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。

6.9 网络安全

a) 结构安全
   1) 应保证主要网络设备和通信线路冗余，主要网络设备业务处理能力能满足业务高峰期需要的 1 倍以上，双线路设计时，宜由不同的服务商提供；
   2) 应保证网络各个部分的带宽满足业务高峰期需要；
   3) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；
   4) 应绘制与当前运行情况相符的网络拓扑结构图；
   5) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段，生产网、互联网、办公网之间都应实现有效隔离；

6) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；
7) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机；

b) 访问控制
1) 应在网络边界部署访问控制设备，启用访问控制功能；
2) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；
3) 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；
4) 应在会话处于非活跃一定时间或会话结束后终止网络连接；
5) 应在网络区域边界(互联网区域边界、外部区域边界和内部区域边界)对网络最大流量数及网络并发连接数进行监控；
6) 重要网段应采取技术手段防止地址欺骗；
7) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；
8) 应对拨号接入用户采用数字证书认证机制，并限制具有拨号访问权限的用户数量。
9) 网络设备应按最小安全访问原则设置访问控制权限。

c) 安全审计
1) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；
2) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
3) 应能够根据记录数据进行分析，并生成审计报表；
4) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，保存时间不少于半年。

d) 边界完整性检查
1) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；
2) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

e) 入侵防范
1) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、注入式攻击、IP 碎片攻击和网络蠕虫攻击等；
2) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

f) 恶意代码防范
1) 应在与外单位和互联网连接的网络边界处对恶意代码进行检测和清除；
2) 应定期对恶意代码防护设备进行代码库升级和系统更新。

g) 网络设备防护
1) 应对登录网络设备的用户进行身份鉴别；
2) 应对网络设备的管理员登录地址进行限制；
3) 网络设备用户的标识应唯一；
4) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
5) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

6) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
7) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
8) 应实现设备特权用户的权限分离；
9) 应定期对网络设备的配置文件进行备份，发生变动时应及时备份；
10) 应定期对网络设备运行状况进行检查；
11) 对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端 ；
12) 口开放审批制度；
13) 应定期检验网络设备软件版本信息，避免使用软件版本中出现安全隐患；
14) 应建立网络设备的时钟同步机制；
15) 应定期检查并锁定或撤销网络设备中不必要的用户账号。

7 其他要求

7.1 隐私信息保护

a) 个人网上银行软件需高度重视保护客户个人金融信息，个人网上银行服务使用时必须向客户提示隐私政策条款。要根据有关方面最新要求不断完善客户隐私政策，持续强化客户隐私保护措施，不得泄露、篡改、毁损其收集的个人金融信息；未经被收集者同意，不得向他人提供个人金融信息。
b) 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，开展有关个人金融信息的收集活动。

7.2 权限获取

a) 移动互联网应用个人信息收集活动，主要依据《信息安全技术个人信息安全规范》的“个人信息安全基本原则”，遵循权责一致、目的明确、最少够用、选择同意、公开透明、确保安全六个原则。
b) 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。
c) 需向用户明示申请权限的目的、方式和范围，申请的权限应具有合法、正当、必要、明确的收集使用目的和业务功能。
d) 不申请打开无关个人网上银行应用使用的权限。只获取满足业务功能所必需的最少类型和数量的权限，自动申请权限的频率不超过业务功能实际所需的频率。

8 技术先进性

采用前后端分离技术， 分开操作，分开部署，解除前端展示和后台处理的耦合，降低了维护的难度。

前端采用成熟的 VX 框架，提供稳定的服务和个性化的设置。结合 angulerjs 进行页面设计与开发。

后台采用成熟的 OSGI 框架，提供系统级架构和服务。

9 创新与前瞻性

前端采用自主框架，提供成熟解决方案。后台采用自主研发框架，提供成熟服务和解决方案。

手机崩溃日志记录：部分机型存在兼容性问题，存在崩溃、闪退等情况。

手机端可记录相应错误信息，提供排查依据。满足当前需求情况下，做功能升级设计。为满足更多客户需求进行优化与开发。

支持通过柜台和电话进行 LPR 转换业务。为爱心人士提供更加便捷爱心捐赠渠道。

助力打赢新冠肺炎防疫战，中银富登推出两款专项产品支持企业复工。抗疫贷用于支持承担防疫物资生产、民生保障等重要社会只能推出的专项贷款；复工贷是面向已复工或拟复工的小微企业、农户等客户，为支持企业采购原料、产品销售等复工复产活动推出的专项贷款。

参考文献

【1】《银行业客户服务中心基本要求》(GB/T 32315-2015)

【2】《信息安全技术 个人信息安全规范》(GB/T 35273-2015)

【3】《个人金融信息保护技术规范》(JR/T 0171-2020)

【4】《网上银行系统信息安全通用规范》(JR/T 0068-2020)

【5】《金融行业信息系统信息安全等级保护实施指引》(JR/T 0071-2012)

【6】《中华人民共和国标准化法》

【7】《金融业标准化体系建设发展规划（2016-2020 年）

【8】《市场监管总局等八部门关于实施企业标准“领跑者”制度的意见》