ICS 03.060
CCS A 11

Q/CMBC

中 国 民 生 银 行 企 业 标 准

Q/CMBC 007—2023
代替 Q/CMBC 007—2022

中国民生银行网上银行服务标准

Enterprise standard of internet banking service of China Minsheng Bank

2023 - 11 - 15 发布　　2023 - 11 - 15 实施

中国民生银行　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替Q/CMBC 007－2022《中国民生银行网上银行服务标准》，与Q/CMBC 007－2022相比，除了编辑性改动外，主要的变化为：

a) 增加了第 4.1.5 反电信网络诈骗治理、第 4.1.6 客户端环境、运行状况、操作行为监测、第 4.1.7 仿冒钓鱼应用监测、第 4.1.8 设备运行环境可信监测、第 4.1.9 用户行为可靠监测、第 4.1.10 欺诈人群信息监测；

b) 在第 5.2.3 条中调整网上银行响应速度；

c) 在第 6.2 条中增加了处理用户投诉要求。

本文件由中国民生银行股份有限公司提出并归口。

本文件起草单位：中国民生银行股份有限公司。

本文件主要起草人：刘衍波、陶江、蔡丹平、崔宇程、石菁菁、吴欣、李晓东、楼晔、虞刚、梁国勇、李娜、谢军、王晓晨、宋宏、臧涵博、李晓、林潇、张洛平、温彦杰、袁丽欧、袁靖、陆文鹏、王广驰、刘辉、赵欣光、顾晶晶、王蓓、龚正、谢燕。

本文件及所替代文件的历次版本发布情况为：

——2019 年首次发布 Q/CMBC 001—2019；

——2020 年第一次修订 Q/CMBC 007－2020，代替 Q/CMBC 001—2019；

——2021 年第二次修订 Q/CMBC 007－2021，代替 Q/CMBC 007—2020；

——2022 年第三次修订 Q/CMBC 007－2022，代替 Q/CMBC 007—2021；

——本次为第四次修订。

引　言

近年来，伴随金融科技的快速发展，网上银行已经成为银行业面向最终客户主要的服务渠道。然而，由于互联网自身固有的风险特性导致网上银行服务存在一些诸如信息泄露、资金损失、网上银行服务交易纠纷难以有效解决等问题和风险。在这样的情况下，提升网上银行的服务质量对整体提升我国银行业的服务水平意义重大。

为提升中国民生银行网上银行服务标准和服务水平，增加网上银行服务领域的标准供给，促进金融风险防控、消费者权益保护，中国民生银行发布《中国民生银行网上银行服务标准》，对发挥企业标准引领质量提升、促进消费升级和推动金融业务转型升级等方面具有重要意义。

本文件参照国家、金融行业相关标准，根据业界当前的实践，采用半形式化的方法给出了网上银行服务的主要服务功能及属性，主要涉及服务安全性、客户体验、创新及前瞻性、实施保障四个方面，旨在明确中国民生银行网上银行服务企业标准，促进网上银行规范、健康发展。

中国民生银行网上银行服务标准

1 范围

本文件规定了本行网上银行服务企业要求，明确了网上银行服务安全、客户体验、创新及前瞻性标准，确立了网上银行服务实施保障机制。

本文件适用于本行所有境内机构的网上银行服务，包括通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向客户提供的网上金融服务，包括由本行直接提供的网上银行、手机银行、银企直联等服务。

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。

ISO/IEC 18036:2003 Information technology-Icon symbols and functions for World Wide Web browser toolbars

GB/T 1.1—2020 标准化工作导则 第1部分：标准化文件的结构和起草规则

GB/T 19000－2016 质量管理体系 基础和术语

GB/T 27912－2011 金融服务 生物特征识别 安全框架

GB/T 32312－2015 银行业客户服务中心服务评价指标规范

GB/T 35273－2020 信息安全技术 个人信息安全规范

GB/T 39786－2021 信息安全技术 信息系统密码应用基本要求

GM/T 0029－2014 签名验签服务器技术规范

GM/T 0030－2014 服务器密码机技术规范

JR/T 0068－2020 网上银行系统信息安全通用规范

JR/T 0071.1-4—2020 金融行业网络安全等级保护实施指引 第1-4部分：基础和术语、岗位能力要求和评价指引、培训指引

JR/T 0118－2015 金融电子认证规范

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

网上银行 internet banking

商业银行等金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供网上金融业务的服务。

[JR/T 0068—2020，定义3.1]

3.2

Web 浏览器 web browser

向因特网服务器发起请求并显示服务器返回的信息的客户机程序。
[ISO/IEC 18036:2003，定义4.5]

3.3

APP (application)

基于软件的提供部分或全部服务的机制。

3.4

API (application programming interface)

软件系统不同组成部分衔接的约定。

3.5

服务 service

至少有一项活动必需在组织和客户之间进行的组织的输出。

3.6

客户 customer

已经或将要发生直接交易关系的对象。
注：在本文件中，顾客与客户视作同义词，并均可简称为客户。

3.7

产品 product

在组织和顾客之间未发生任何交易的情况下，组织能够产生的输出。
[GB/T 19000—2016，定义3.7.6]
注：在本文件中，仅考虑通过网上银行的服务向顾客提供产品和支撑产品运作的情况。

3.8

客户满意度 customer satisfaction

客户期望值与客户体验的匹配程度，是客户在感知银行服务效果并与其期望值相比较后得出的指数。
[GB/T 32312—2015，定义2.5]

4 服务安全性

4.1 基本安全要求

4.1.1 安全技术标准

4.1.1.1 安全技术通则

网上银行系统安全应符合GB/T 35273—2020、GB/T 27912—2011、GM/T 0030—2014、GM/T 0029—2014、JR/T 0068—2020、JR/T 0071.1-4—2020、JR/T 0118—2015、JR/T 0171—2020等相关标准

的要求，应至少满足GB/T 39786—2021中对信息系统第三级密码应用的基本要求，并在国家标准和行业标准的基础上，增加包含客户端、网络、服务器、与外部系统通讯和二维码/条码及个人金融信息保护在内的安全标准。

4.1.1.2 客户端安全

客户端安全指PC端和移动端的应用安全，包括以下内容：

a) 手机银行 APP 宜在终端具备安全能力的情况下优先支持 Fast IDentity Online (FIDO) 协议，支持指纹、人脸等认证方式，通过 FIDO 协议实现基于终端设备的认证；在终端不具备安全能力的情况下宜下发用户白盒密钥到客户端设备，实现交易过程中对终端的可信验证；
b) 客户端应对服务器数字证书的完整性合法性校验，采用在客户端预埋验签公钥对数字证书签名进行校验，防止中间人攻击；
c) 图片验证码不能在客户端生成，不能通过报文传输验证码中的文本信息；
d) 手势密码不应保存在客户端，应以加密形式保存在服务器端。

4.1.1.3 网络安全

网络安全指客户端与服务器端间网络安全，包括以下内容：

a) 在 SSL 加密链接的基础上，手机 APP 应增加对交易报文的加密，防止敏感信息泄露及篡改；
b) 企业网上银行应支持基于国密算法的 SSL 协议。

4.1.1.4 服务器端安全

服务器端安全指服务器端应用程序安全，包括以下内容：

a) 应用系统应具有防请求重放机制；
b) 对于文件上传和文件下载，应注意控制文件类型，限制文件目录的权限，防止前端越权访问；
c) 服务端在验证短信验证码时，应使用客户预留的可信手机号码进行校验，防止越权使用；
d) 对于短信验证码认证与交易操作分步执行的情况，应在认证通过后分配认证标识，与用户信息绑定，且使用一次后失效。

4.1.1.5 与外部系统通讯安全

外部系统指非民生银行系统，网上银行与其连接应保证安全性，包括以下内容：

a) 应实现对商户系统本身客户的身份认证和交易安全；
b) 客户发起的交易真实性和合法性应通过外部系统平台进行保证，通过外部系统发起的交易指令使用数字证书进行数字签名；
c) 银企直联代理应使用数字证书在合作企业客户与民生银行间建立双向 SSL 安全通道，保证数据传输的完整性、保密性；
d) 在通过互联网进行通讯时，应建立外部系统与民生银行服务器间双向 SSL 认证通道，并验证通讯证书与商户编码的签约关系；
e) 为商户提供 API 功能时，应使用密钥协商机制，保证移动应用客户端与我行服务器交互时的数据安全；
f) 应为商户提供数字证书申请服务和数字证书安全应用接口，对交易数据做数字信封加密和数字签名，保护数据安全和防止商户对交易行为进行抵赖。

4.1.1.6 二维码/条码

二维码/条码相关的规范包括：

a) 二维码/条码应采用标记化技术，码值本身不应含客户及账户敏感信息，关联关系应存放到后台系统，以防止信息泄露；
b) 二维码/条码应设置使用次数和有效期；
c) 二维码/条码支付业务开通时，应对客户身份进行验证确保客户本人操作，对客户端登录状态进行校验，确保在有效登录期；
d) 二维码/条码交易时，应根据支付限额验证相应的安全工具，小额交易可以参考相关规定减少安全工具校验，大额交易宜采取双因素安全校验。

4.1.2 安全管理

应设立专门的安全管理机构，对网上银行的安全制定相关制度办法，包括以下内容：
a) 应明确安全管理机构和其他各相关机构的职责范围、工作流程和沟通协调机制；
b) 应按照系统应用架构、系统使用人员、访问终端类型、发布方式等方面进行安全评估，确定网上银行的安全风险等级；
c) 应为网上银行系统建立安全评估机制，对新系统上线和系统变更制定全生命周期的安全评估机制，具备安全事件的应急处理能力；
d) 应为网上银行系统建立源代码安全检查机制，对缺陷整改情况进行跟踪；
e) 应为网上银行系统建立定期安全渗透测试和漏洞检查机制，对漏洞库进行统一管理，并持续跟踪漏洞修复状况；
f) 应为网上银行建立安全风险分析及处理机制，针对用户异常行为和系统攻击可以进行追踪溯源。

4.1.3 业务运作安全

4.1.3.1 身份认证

网上银行服务的开通应由客户本人进行申请，开通时，应验证客户的真实身份，核实客户的意愿。

4.1.3.2 安全工具的申领

客户申请USB KEY、动态令牌等安全设备时，应持有效身份证件办理，采取将设备序列号与客户信息进行绑定的措施，确保设备与客户一一对应，如果安全设备丢失，需客户持有效证件重新办理，原有安全设备和客户绑定关系解除。

4.1.3.3 交易安全策略

a) 非客户本人同名账户之间的资金类交易，应设置与场景匹配的限额控制，如单日累计金额限制、单日累计笔数限制、年度累计金额限制等；
b) 宜提供安全账户锁的功能，允许客户设置转账、消费、取现的限额锁，以及跨境锁、夜间锁，以及非常用地锁等。

4.1.4 个人信息保护

应对客户的账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、信贷信息和其他反映特定个人金融信息进行严格保护，制定相应的相关管理制度，在管理制度中对客户个人信息等进行明确分类分级定义。

个人信息保护措施应覆盖个人信息收集、存储、传输、使用、销毁完整的个人信息生命周期环节，具体包括：

a） 个人信息的收集，应符合以下原则：
   1） 应通过隐私政策等方式向客户明示网上银行运行过程中收集、使用用户个人信息的内容、目的、方式和范围等；
   2） 在客户端上输入密码等敏感信息时，不能以明文的方式显示在屏幕上；
   3） 在客户端上输入个人信息时，用户输入的数据应不能被其他程序非法获取;
   4） 不委托或授权无金融业相关资质的机构收集客户敏感信息。
b） 个人信息的存储，应符合以下原则：
   1） 客户端上不能存储敏感个人信息及其密文，敏感个人信息及其密文在使用后应立即清除。客户端存储一般个人信息时，应进行加密处理；
   2） 服务器存储个人信息，应根据个人信息自动和非自动处理的特点，制定相应保护策略，包括访问控制、权限设置、密钥管理等，防止个人信息的不当使用、毁损、泄露、删除等；
   3） 应定期备份存储的个人信息，保证备份、恢复的完整性、可靠性和准确性。
c） 个人信息的使用，应符合以下原则：
   1） 敏感个人信息中的个人认证信息不能以任何形式下发到客户端。认证信息的比对只能在服务器进行。敏感个人信息中的个人身份信息在下发至客户端之前，应屏蔽个人身份信息中不可猜测的一部分，被屏蔽部分使用统一的符号替代；
   2） 采用专门用于测试的测试账户进行开发测试，真实个人信息不得用于开发测试。
d） 个人信息的传输应对传输个人信息的通信过程中的整个报文或会话过程进行加密；
e） 个人信息的销毁，应符合以下原则：
   1） 应制定严格的个人信息销毁制度，确保应记录个人信息的相关的文档、介质得到及时、有效的销毁，个人信息销毁前应得到相应的授权；
   2） 对于以下保存到期或已经使用完毕的个人信息，均应建立严格的销毁登记制度：纸质、光盘、磁带及其它可移动的数据存储载体等介质中存储的个人信息；报废设备或介质中存储的个人信息； 其他超过保存期限需销毁的个人信息；
   3） 应保证存储敏感个人信息的介质在销毁后，信息不可恢复；
   4） 对于所有需销毁的个人信息，应在双人控制、监督人员在场情况下，采取有效措施，及时妥善销毁。

4.1.5 反电信网络诈骗治理

a）需建立并持续完善反电信网络诈骗风控体系，建立基于事前、事中、事后的风险预警监控系统，建立线上与线下联动处置机制，实现风控策略与客户体验动态均衡；

b) 需建立并完善风险监控模型，识别并区分盗窃与诈骗行为，区分犯罪份子域受害人等不同人群，结合客户风险等级与交易行为风险等级，在事前、事中、事后对客户采取动态管理处置，对客户形成漏斗式风险逐层过滤，保障客户资金安全；

c) 需建立多维度交易核实与核验方式，如风险提示、认证提级、远程认证、延迟支付结算、限额调整、交易阻断、账户止付等方式进行动态处置；

d）需建立线上渠道与线下网点联动机制，在银行内部形成风险共识，及时通过线上拦截加线下劝阻的方式进行联防联控，在保障客户资金安全的同时同步增强客户体验；

e）需定期进行反电信网络诈骗宣传工作，在门户网站或官方渠道发布反电信网络诈骗宣传安全提示。

4.1.6 客户端环境、运行状况、操作行为监测

a）需对客户端应用软件具备环境的检查能力，检查的范围应包括：系统是否安装网上银行安全控件、系统是否越狱或ROOT、程序运行环境是否可信等，并能向后台系统反馈设备环境信息等；
b）需对移动金融客户端运行安全状况进行检测并向后台系统反馈，对设备的运行安全情况进行识别和监测，并建立相应的风控策略保障其客户端运行环境的安全性；
c）针对移动金融客户端的用户行为进行监控，建立用户操作行为安全基线，实时预警用户不可控的行为，一旦发生预警，与客户主体进行联系，验证其客户身份及操作行为的真实性；
d）需在门户网站或官方渠道发布移动金融客户端环境安全的提示。

4.1.7 仿冒钓鱼应用监测

需对移动应用市场进行7*24小时监测，及时发现仿冒银行的恶意链接、钓鱼网站或伪冒第三方移动应用。

4.1.8 设备运行环境可信监测

需对移动金融客户端用户环境风险进行监测，及时针对木马病毒、网络攻击、异常IP、地理位置、设备ID、MAC等多维度信息进行实时采集、识别、预警、响应。

4.1.9 用户行为可靠监测

需对用户的交易行为进行事前、事中、事后的全过程监控，对异常交易行为进行威胁预警与风险策略保护。

4.1.10 欺诈人群信息监测

需充分利用内部以及外部公安涉炸、黑产及司法失信等信息，通过数据应用、数据获取与数据分析有效识别用户身份识别效率与准确度。

4.2 服务连续在线可信性

为了保障服务连续在线可信性，规定以下标准：
a） 网上银行系统服务时间应满足 7×24 小时不间断运行；
b） 应配备 7×24 小时运维应急人员，建立应急管理制度和团队，能积极响应生产紧急事件；
c） 网上银行系统可用率应≥99.99%；
d） 网上银行相关系统（手机银行系统、新网银系统、直销银行系统）系统恢复时间（RTO）应≤30 分钟；
e） 应急预案更新率=100%，演练覆盖率=100%。

4.3 增强身份认证要求

4.3.1 防范伪造攻击技术

4.3.1.1 环境检测

客户端应用软件在运行时具备对运行环境的检查能力，检查的范围应包括：系统是否越狱或 root、程序运行环境是否可信（例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环境信息等。

4.3.1.2 抗攻击能力

a） 移动金融客户端应具备抗攻击能力，包括但不限于抵御静态分析、动态调试、保持自身完整性、真实性，防范客户端程序被篡改及注入；

b） 移动金融客户端代码应使用代码加壳、代码混淆、检测调试器、加壳等安全手段对客户端应用软件进行安全保护，防止客户端程序被逆向分析；

c） 移动金融客户端应用软件应进行签名，签名证书能有效标识应用软件的来源和发布者，保证客户所下载的客户端程序来源于所信任的机构；

d） 应采取渠道监控等措施对仿冒客户端程序进行监测；

d） e） 移动金融客户端应具有已知漏洞的防范能力，当发现客户端存在重大安全缺陷或安全威胁时，应采取必要措施对用户进行警示或拒绝交易。

4.3.2 增强身份认证

网上银行应支持多种增强身份认证方式，并根据不同场景和交易限额匹配不同认证手段，包括以下内容：

a） 网上银行应支持多种身份认证方式，如静态密码、短信验证码、动态令牌、USB key 等。移动端还应支持手机 U 宝、手势密码、FIDO 指纹/人脸/声纹等安全认证方式；

b） 资金类交易的开通必须由客户本人到柜台申请或通过远程银行申请，或通过 USB Key、动态令牌等安全设备在各线上渠道自行开通；

c） 应采取交易验证强度与交易额度相匹配的身份认证措施，提高交易的安全性。高风险业务应采用双因素身份认证。双因素身份认证由以下三种身份认证方式中至少两种组成：一是客户知悉的要素，如静态密码等；二是客户本人持有并特有的，不可复制或者不可重复利用的要素，包括但不限于物理介质、电子设备、数字证书等；三是客户本人的生物特征要素，如指纹、虹膜、声纹等。应确保采用的交易验证要素相互独立，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；

d） 使用的短信验证码应与交易要素进行绑定，并采用支持国产密码算法的硬件加密设备生成；

e） 手势密码可在系统登录、应用从后台返回等场景中使用，不能在以下场景中作为验证用户身份的凭据，包括交易验证、修改登录密码、开户等。

4.4 风险控制能力

网上银行系统应对交易事前、事中及事后的风险防控提出规范和要求，包括以下内容：

a） 应对交易过程进行账户级风险识别与干预，对于包括用户注册、登录、支付、转账、绑卡、贷款等风险进行识别，防范潜在的非法交易、欺诈交易；

b） 应建立网上银行交易监控的相关系统，能够甄别并预警潜在风险的交易；应建立反洗钱监测平台，并建立可疑交易监测标准，识别包括套现在内的主要洗钱犯罪；应建立业务安全威胁分析预警平台，收集行内客户行为数据以及外部情报，进行客户行为分析，构建客户画像，识别业务安全威胁；宜建立欺诈交易侦测平台，在交易过程中结合欺诈交易风险特征，采取电话、短信等方式进行风险识别与审查；

c） 应根据交易的风险特征建立风险交易模型，有效监测可疑交易，形成客户信息与账户管理、客户账户交易、授信及资产业务等业务类型的风险交易模型，对可疑交易建立报告、复核、查结机制；

d） 应对监控到的风险交易进行及时分析与处置。信用卡中心对于监控到的潜在欺诈交易，应及时进行卡片管控，对于监测到的疑似套现交易，应采取相应的管控措施；网络支付收单商户应开

展事后交易风险分析与处理，依据系统数据进行商户风险非现场巡检；运营风险监控平台应建立处置和评估的分析处置过程，并建立风险事件库，用于模型优化和管理提升。

5 客户体验

5.1 网上银行服务功能

5.1.1 个人客户服务功能

5.1.1.1 账户管理

账户基础服务包括：

a) 本行I类户账户管理服务：包括银行资产总览、余额查询、交易明细查询、账户开户网点查询、电子回单查询、权限管理、密码管理、个人信息变更、账户别名维护、追加/删除下挂账户、账户挂失、账户安全锁、借记卡预约办卡、电子账户在线开户；

b) 本行 II、III 类户账户管理服务：包括 II、III 类账户开户、资产总览，余额查询，明细查询，个人信息变更，账户权限管理，绑定卡变更，密码管理，账户销户等服务。通过合作第三方商户开立的 II、III 类账户功能范围应不超出自有渠道开立账户所提供的范围；

c) 他行账户管理服务：主要包括通过跨行通来完成他行卡资金归集、他行卡账户信息查询等。

5.1.1.2 转账汇款

包括本行同名汇款、跨行汇款，跨境汇款、预约转账、爱心/公益捐款、绑定手机号汇款、II/III类账户和绑定卡之间的出入金等功能。

5.1.1.3 支付服务

包括二维码收付款、NFC移动支付、快捷支付管理、支付历史查询、闪付免密等功能。

5.1.1.4 存款服务

包括结构性存款、特色定期存款、通知存款、定期存款、大额存单等。

5.1.1.5 贷款服务

包括经营性贷款、消费性贷款、贷款计算器等。

5.1.1.6 银行代销产品服务

包括代销理财产品、代销基金、代销保险、贵金属、债券类、银证银期等。

5.1.1.7 投资交易类服务

包括账户交易类、债券类、贵金属类等。

5.1.1.8 非金融增值服务

移动端包括商旅服务、生活休闲、交通出行、积分兑换、特惠商户等。

5.1.1.9 客群专属服务

包括私人银行专属服务、小微银行专属服务、信用卡及直销银行客户专属服务入口。

5.1.1.10 网点联动服务

包括网点信息查询、ATM二维码取现、ATM预约取现、网点预约排号/取现。

5.1.1.11 线上客服类服务

包括在线文本客服、远程视频服务。

5.1.1.12 消息服务类

包括账户动账通知、银行公告、财富资讯、优惠快讯、金融日历提醒等。

5.1.1.13 API 输出业务

通过API接口模式将银行产品及服务输出到合作商户，输出业务包括：账户开立、账户管理、转账支付、财富产品、贷款产品等金融服务。

5.1.1.14 信用卡类服务

a) 账户基础服务：包括账单查询、额度管理、账单寄送、积分查询、账户安全管理、短信通知及账单日管理、账户密码管理等操作；
b) 还款服务：包括已出和未出账单还款、本外币还款、本行和他行卡还款、自定义还款、最低还款和自动还款等操作；
c) 卡片管理服务：包括线上申卡办卡、办卡进度查询、卡片激活、卡密码管理、解绑卡等操作；
d) 借贷服务：包括现金分期、账单分期、自由分期、转账取现、分期查询等操作、按日计息、随借随还等借贷服务。

5.1.2 对公客户服务功能

5.1.2.1 账户管理服务

账户管理服务包括各种查询、对账及回单、单位结算卡等服务，具体如下：

a) 基本查询：财务总览、账户余额查询、交易明细查询、定期存款查询、保证金账户查询、贷款查询等；
b) 其他查询：法透账户查询及还款、凭证状态查询、票据信息查询；
c) 对账及回单：客户回单、网上对账；
d) 单位结算卡。

5.1.2.2 转账汇款服务

转账汇款服务包括基本转账、向个人转账、其他转账，具体如下：

a) 基本转账：行内转账、跨行汇款、预约转账、批量转账；
b) 向个人转账：代发工资、费用报销；
c) 其他转账：缴费类、公益事业捐款、转定期保证金、公积金放款、跨行资金归集、中国证券登记结算、金交所会员入金、期货交易所入金、财税库行缴纳税款、跨境人民币代理汇款、国库集中支付、期货公司资金划转、跨行支付状态查询等。

5.1.2.3 票据服务

票据包括电子票据和票据管家两大类服务。

5.1.2.4 现金管理服务

现金管理服务包括集团账户、全球现金管理、场景类服务，具体如下：

a) 集团账户服务、现金池、智能账簿等集团资金管理服务；
b) 全球现金管理：即跨境资金池，实现集团总部及下级成员间的跨境账户管理；
c) 场景类服务：面向行业客户提供的账户管理、支付结算以及信息服务等功能，例如：招标通、回款通、房管通、分销易等产品。

5.1.2.5 对公存款服务

对公存款服务包括存款和同业资金管理两大类，具体如下：

a) 存款类: 包括定期存款、通知存款等产品、大额存单、流动利、随享存；
b) 同业资金管理。

5.1.2.6 银行理财服务

包括固收类、衍生类、权益类、混合类四大类理财服务。

5.1.2.7 投资交易类服务

投资交易类服务包括基金投资、第三方存管、银商转账、银期转账、贵金属交易等服务。

5.1.2.8 商户服务

商户服务主要包括B2B和基金业务商户两大类服务。

5.1.2.9 贸易金融服务

贸易金融服务可分为结售汇及外汇买卖、网上保理、银关税费通、汇出汇款、汇入汇款、进口代收、进口信用证、国内信用证、保函及单一窗口综合服务等服务。

5.1.2.10 网络融资服务

网络融资服务提供流动资金贷款、银行承兑汇票在内的融资贷款等服务。

5.1.2.11 客户专属服务

为特殊客户提供的特色专有功能，只有特定客户可见，如IATA、海淀财政等服务。

5.1.2.12 功能设置类服务

功能设置类服务分为：业务管理及权限设置、渠道签约、其他设置等服务。

5.1.2.13 银企直联服务

向企业ERP系统提供的接口服务，功能可为查询、转账、回单下载、代发工资、费用报销、智能账簿、现金池、票据等。

5.2 网上银行服务性能

5.2.1 网上银行客户体验

5.2.1.1 易用性

网上银行服务易用性应具备以下基本要求:

a) 以客户视角，宜提供客户账户总览、产品筛选、功能搜索、产品推荐等服务功能，使软件更简易、高效地适应用户的使用需求和习惯；
b) 应提供新手引导、新功能上线指引、在线客服，宜提供语音导航方便客户使用；
c) 应在布局合理的情况下，做到输入简单，如提供图像识别自动录入卡面信息、粘贴板自动录入卡号信息等功能；
d) 业务流程应符合具体客户需求，最大程度减少操作步骤，使客户高效、直接完成功能操作。

5.2.1.2 舒适性

网上银行服务舒适性应具备以下基本要求:

a) 应符合相关设计规范，设计风格协调统一，信息表达简洁和美观；使用标准配色、合理运用色彩含义、色彩对比；
b) 提示文案应环境贴切，与现实匹配；应使用标准字体、字号；使用日常、自然的语言与用户进行交流；
c) 应融入情感化设计与用户进行情感交流，如有专属卡通形象作为与客户沟通纽带。

5.2.1.3 便捷性

网上银行服务便捷性应具备以下基本要求:

a) 应做到功能易找，如支持客户定制页面内容及功能入口、常用功能前置、提供快捷金融小应用、交互层级扁平、栏目分类科学、导航清晰；
b) 操作所需步骤、流程应简洁有序，任务流程连贯闭环、无断点，功能具有接续性，反馈应友好、指引应清晰，如申请类、注册类服务有进度指示；
c) 应提供不同客群专属版本，如小微银行专版、私人银行专版；可根据服务客群，提供专属服务入口；
d) 宜提供线上线下一体化服务，如扫二维码支付、扫二维码取现、网点预约排号等服务；
e) 应提供丰富的生活周边服务，如生活缴费、网上购物、出行服务等服务。

5.2.1.4 易访问性

网上银行服务易访问性应具备以下基本要求：

a) APP 应支持主流应用商店下载、线下扫二维码下载等下载方式；
b) 移动银行端应具备指纹登录、手势登录、人脸登录等快捷登录方式；
c) 应提供 APP、WEB 浏览器、社交平台公众号等多种访问方式；
d) 银行网点宜提供自助服务终端，方便客户登录、下载、开通网上银行服务。

5.2.2 网上银行闪退率要求

网上银行面向公众的主流APP的闪退率应≤0.05%。

5.2.3 网上银行响应速度

页面开始浏览到接受到最后一个数据包之间的时间差不宜超过5秒。

5.2.4 网上银行总下载字节要求

整个浏览过程中IE内核的总下载量不宜超过10000KB。

5.3 客户代表行为规范

5.3.1 职业守则

客服代表职业守则主要包括：

a) 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；
b) 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；
c) 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；
d) 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；
e) 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；
f) 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，都应时刻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：

a) 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；
b) 客服代表接通电话时应主动倾听，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；
c) 客服代表接通电话时应主动服务，有较强的语言表达技巧和沟通能力，思路清晰，恰当引导客户，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；
d) 客服代表接通电话时应服务意识强，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：

a) 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；
b) 客服代表应养成良好的通话习惯，保持恰当的语速和音量，通话时语气和蔼，吐字清晰、流畅自然；
c) 服务用语应礼貌、规范，提倡讲普通话，必要时可提供英语服务，创造良好的沟通环境。杜绝使用蔑视语、烦躁语。客服代表应在客户长时间等待或客户等待后对客户表示歉意，恰当的使用“请、您、谢谢、对不起、请稍等”等礼貌用语。

5.3.4 业务能力

客服代表业务能力要求主要包括：

a） 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；
b） 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，避免不必要持线；
c） 客服代表应对于超出解答范围的问题，主动、客观记录客户问题，及时反馈客户意见及投诉情况，并在必要时跟进。

5.3.5 操作合规

客服代表操作合规要求主要包括：
a） 应严格执行各项业务操作规程，按制度规定执行；
b） 为客户办理金融交易时，须认真审核客户身份、交易信息等重要内容，不得出现错办、漏办、超范围办理等不规范现象。

5.3.6 仪容仪表

视频客服代表仪容仪表规范要求包括：
a） 客服代表应统一着装，衣着整洁，礼仪规范；
b） 客服代表应友善对待客户，行为文明、举止大方。

5.4 客户服务响应

客户服务应建立全面的服务指标管理体系。通过质量、效率及客户满意度等指标的制定、考核评估、指标结果反馈、沟通辅导等一系列流程，实现数据化闭环管理，促进整体服务指标及人员综合能力的稳步提升。客户服务响应指标包括：
a） 服务效率：通过接通率、服务平均响应时间两项指标对服务效率进行测量。具体要求如下：
1) 电话服务平均响应时间：即转接人工客服后到人工客服接通平均时间，此项指标要求≤15秒；
2) 线上客服平均响应时间：即客户发出文本指令后服务响应时间，此项指标要求≤5 秒；
3) 电话客服接通率：即人工接起电话量占所有请求人工服务的客户数量比例，此项指标要求≥95%。
b） 服务体验：通过客户满意度测评进行服务体验测量。具体要求如下：
客户满意度：即通过 IVR 方式在服务结束后进行客户满意度测评，测量客户对客服中心整体服务的满意程度，此项指标要求达到 98%；其中，客户满意度公式为：客户满意度公式为：客户满意度=（1-客户不满意量）/总参评客户数量。
c） 服务时间：客户服务时间应满足 7×24 小时；
d） TCP 时间：<= 100ms；
e） 整体速度：> 500kb/s（不考虑客户本身网络速度限制）。

6 创新及前瞻性

6.1 创新机制

应规范中国民生银行创新管理工作，完善创新管理体系，提升自主创新能力，推动创新业务合规、有序、健康发展。网上银行聚焦客户服务体验，通过千人千面智能服务、金融产品的数字化创新、 IT 技术升级、业务流程改造等网络金融领域创新，提供前沿性、创新性的网络金融服务能力。根据创新内容分为产品创新、模式创新、技术创新。

6.2 服务（产品）创新

6.2.1 创新内容

服务（产品）创新包含以下内容：

a) 应使用统一用户体系，实现一套账户密码登录手机银行 APP、网银、信用卡全民生活 APP 等网上银行服务平台；
b) 针对不同客群的差异化服务需求，应提供面向专属客群的差异化版本服务能力；
c) 宜建设客户开放体系，实现对本行客户、他行客户、互联网客户的平台服务能力；
d) 宜提供远程视频服务，借助高速音视频传输、数据交互、身份识别等技术，为客户提供线上业务办理、线下物流实物交付、网点专人或移动上门服务支持和“端到端”服务流程跟进等全方位服务；
e) 应借助大数据分析，以智能化的方式区分个体差异，支持在多个版块及交易页面的广告区域、投资理财产品的推荐区域等千人千面精准营销，可根据客户属性（如地区、资产情况等）推送特色营销活动及个性化的产品；
f) 应根据个人客户个性化的风险偏好，实现根据交易时间、地点、金额、渠道等维度进行客户自定义的支付安全设置；
g) 应提供机器人智能应答服务，通过文字语意分析等技术，提供智能话术应答；
h) 宜将生物识别技术与网上银行服务高度融合，为个人客户提供指纹支付和登录、人脸识别登录及转账、手势密码、虹膜支付等生物识别应用；
i) 宜将前沿性技术与网上银行服务场景结合，提供语音识别、图像识别（OCR）等服务功能;
j) 针对零售和小微存量浮动利率贷款客户，应提供线上办理 LPR 利率转换的服务能力，实现待转换贷款数据查询、转换操作;
k) 聚合行内外内容资源，为客户提供风险防范、理财宣讲等非金融服务能力。
l) 应在官方网站、移动客户端公布我行 7*24 小时全行投诉受理电话 95568；投诉通讯地址：北京市西城区复兴门内大街 2 号；服务监督邮箱：95568server@cmbc.com.cn。在官方网站首页设置“投诉渠道”专栏，公示投诉流程以及信用卡、小微、个人、公司的专线投诉热线。针对投诉事项的紧急程度、重要程度、潜在风险区别界定投诉级别，按照不同级别的投诉，分别设置不同的处理时限，一般情况下不超过 1 至 5 个工作日，如遇情况复杂的疑难投诉经领导审批通过后，可延长投诉处理时限，最长不超过 15 日，本着以客户为中心、尽快解决客户诉求的原则，及时妥善处理客户的投诉，并定期进行投诉分析，不断提高客户满意度。

6.2.2 创新实践

宜提升安全管理和风险防控能力，建设民生网上银行客户端，支持民生各网上银行版本，解决Windows系统停止支持IE浏览器导致的浏览器兼容性问题，提升网上银行安全防护和客户体验水平。

6.2.3 适老化及无障碍化使用

企业网银适老化及无障碍化使用应满足要求：视觉设计主要以清晰可辨为目标，应具备大字体、大图标、文字高对比度、页面放大及缩小等功能。

6.3 模式创新

模式创新包含以下内容：

a) 可通过 API 技术搭建开放银行服务平台，借助“嵌入场景、输出金融”的创新模式，实现将 II、III 类账户输出到合作商户，提供账户开立、账户管理、转账支付、财富产品、贷款产品等功能嵌入第三方；
b) 可提供信用卡虚拟化业务模式，实现线上实时申卡、办卡、激活等功能，支持虚拟卡实体化、无卡支付、消费及借贷的一站式用卡体验；
c) 可提供直销银行服务，通过提供在线 II、III 类账户服务和专属金融产品，客户全流程无需到网点办理，可以使用任何一家银行借记卡作为绑定账户，便捷地在线完成转账支付，购买投资理财产品，申请贷款等银行业务。

6.4 技术创新

6.4.1 技术创新内容

技术创新包含以下内容：
a) 针对互联网级别的海量客户、海量服务、海量数据，应在基础架构上进行分布式架构转型并商用于核心生产系统；
b) 应使用大数据技术，包含但不限于：风险与欺诈分析、运营优化、市场洞察、舆情分析、智能获客等方面；
c) 可使用指纹、人脸、虹膜、声纹等生物识别技术认证方式，增强身份认证安全性和认证手段多样性；
d) 宜建设自然语言处理平台，结合 AR/VR、人工智能技术，向网银、手机银行等网上银行服务平台提供服务支撑；
e) 宜实施基础设施 IaaS 云化改造和容器云 PaaS 建设，宜推进网上银行相关应用云端化；
f) 运维部署采用两地三中心多活体系，保证业务连续可用。

6.4.2 技术创新实践

民生银行基于分布式技术，完成了银行核心系统的无缝升级改造，基于大数据风控模型，在转账、贷款、支付等业务场景增加了业务风险处置，在端侧增加了威胁感知能力。综合应用指纹、人脸、虹膜等生物识别技术，以及短信、sim卡认证等技术，在渠道侧形成了可根据具体业务进行灵活配置的安全验证工具。在手机银行推出了AR看金业务，运用AR技术让用户在线体验实物金佩戴效果。

7 实施保障

7.1 组织机构保障

7.1.1 网上银行业务牵头部门

网上银行业务牵头部门的具体职能包括：
a) 统筹管理全行网上银行业务，制定和组织实施我行网上银行业务发展规划；
b) 负责网上银行各类渠道服务的统一管理；
c) 负责网上银行业务统一的需求统筹、平台建设、敏捷开发、流程管理、风险管理、数据挖掘、营销策划等；
d) 负责网上银行业务管理、制度建设、监管报批、安全建设、反洗钱等职责。

7.1.2 网上银行支持保障部门

网上银行支持保障部门的具体职能包括：

a) 应由信息科技部门负责信息科技建设管理体系规范，负责网上银行业务相关系统建设管理及运营维护工作；
b) 应由运营管理部负责网上银行柜面业务相关的账户管理、资金清算、账务处理、客户服务的操作流程审定与发布、后台业务集中运营等；
c) 应由审计部门负责对全行网上银行业务进行相关审计；
d) 应由公司、零售、金融市场等业务条线部门负责各自领域的产品线上化管理。

7.1.3 分行机构

分行应贯彻落实总行网上银行业务发展规划和工作部署，执行各项网上银行业务管理制度，组织开展网上银行产品推广、市场拓展、业务检查、安全教育、同业调研等工作，配合总行开展风险事件协查处理。

7.2 管理制度

7.2.1 产品研发类制度

应制定产品研发类制度，以确保网上银行相关的产品研发资源合理安排，规范研发项目的管理流程，提高研发效率，具体包括：产品创新制度、项目评审制度、项目管理制度，项目开发规范、设计规范、后评估机制等。

7.2.2 测试投产类制度

应制定测试投产类制度，以确保网上银行相关的项目安全、高效、顺利实施，具体包括：测试过程管理规范、测试质量管理规范、系统投产规范等。

7.2.3 生产运维类制度

应制定生产运维类制度，以确保网上银行相关的生产安全与运维规范，具体包括：生产运维规范、配置规范、变更规范，以及系统、网络、机房、数据、安全等配套管理规定。

7.2.4 业务管理类制度

网上银行各类服务渠道均应制定业务管理办法，以规范其部门职责、业务范围、经营模式、风险管理等。网上银行提供的各类线上业务应遵循相关产品负责部门提供的产品管理办法，包括但不限于转账汇款、支付缴费、存款类、贷款类、投资交易类等。

7.2.5 应急响应类制度

应制定应急响应类制度，以确保网上银行相关业务具备应急响应措施，妥善处理各类突发事件，保证业务的连续性，具体应包括：信息系统、反洗钱、流动性、消费者权益保护等突发事件应急预案、业务连续性应急预案、生产系统事件管理办法等。

7.3 企业标准宣传及实施机制

7.3.1 宣传与培训机制

应确定企业标准的管理部门，建立总行、事业部、分行的分层宣传与培训机制，确保层层传导。

全行各级机构应针对标准定期组织开展多层次的业务培训和文化建设活动，提升相关人员的专业知识和标准服务意识。

全行各级机构应认真学习企业标准，管理部门应对各部门进行业务培训，有条件的宜进行考试及认证工作，按要求落实企业标准要求。

应将企业标准上传公示至标准信息公共服务平台，并将企业标准纳入行内广告投放与宣传的计划范围内。

7.3.2 实施监督机制

全行各级机构应制定贯彻落实企业标准的工作机制，建立严格的实施监督制度，各级机构可将企业标准分解指标，纳入相关团队的考核。

全行各级机构应将对企业标准的执行情况定期上报，企业标准的管理部门应对各机构情况进行汇总和通报，对出现不符合标准的情况，应及时督导整改。

企业标准的管理部门应根据行内业务实际的发展情况，每年对标准进行维护和更新，并将最新版的标准进行公示和行内发布。

参 考 文 献

[1]GB/T 32315—2015　银行业客户服务中心基本要求
[2]GB/T 29799—2013　网页内容可访问性指南
[3]GB/T 37668—2019　信息技术互联网内容无障碍可访问性技术要求与测试方法