ICS 03.060
CCS A 11

团　体　标　准

T/NIFA 12-2022

网上银行服务 基本要求

Internet banking service — Basic requirements

2022-6-9 发布　　2022-6-9 实施

中国互联网金融协会 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》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网金融协会提出。

本文件由中国互联网金融协会归口。

本文件起草单位：中国互联网金融协会、中国工商银行股份有限公司、中国邮政储蓄银行股份有限公司、中国民生银行股份有限公司、重庆农村商业银行股份有限公司、蚂蚁科技集团股份有限公司、中国建设银行股份有限公司、大连银行股份有限公司、杭州银行股份有限公司、中国银行股份有限公司、深圳前海微众银行股份有限公司。

本文件主要起草人：陆书春、朱勇、易琮、王新华、刘燕青、赵鹏辉、梅超、徐晓群、马亮、胡小龙、李琳、沈澍、娄涵、戚扬、陆文鹏、杨峰、田成志、陆碧波、彭晋、吴猛、刘洋、徐皓、樊存智、洪慧、沈勤、曹克、张昊、孙雯、廖静骁。

引　言

近年来，伴随金融科技的快速发展，网上银行迭代创新与时俱进，网上银行服务越来越受到企业和个人客户的青睐。为契合国家战略导向和社会发展需要，坚持以人民为中心，贯彻新发展理念，助力高水平科技自立自强，落实《金融标准化“十四五”发展规划》，在总结网上银行服务企业标准“领跑者”活动的基础上，提出网上银行服务基本要求，以此指导和促进中国银行业网上银行服务的高质量发展。

本文件旨在为银行业金融机构开展网上银行服务提供指导，促进网上银行服务能力持续提升，在服务体验方面使网上银行服务更智能、更便捷、更安全和更优质，不断满足人民群众对金融服务的获得感和安全感。

网上银行服务 基本要求

1 范围

本文件提出了银行业金融机构开展网上银行服务的基本要求，规定了开展网上银行服务的服务形态、服务功能、服务体验、服务安全、服务保障、服务创新的要求。

本文件适用于银行业金融机构网上银行服务的设计、建设和优化，也可为银行业金融机构编制网上银行服务企业标准提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25000.10 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型

GB/T 31186—2014（所有部分） 银行客户基本信息描述规范

GB/T 32315—2015 银行业客户服务中心基本要求

GB/T 32319—2015 银行业产品说明书描述规范

GB/T 35273—2020 信息安全技术 个人信息安全规范

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

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

JR/T 0068—2020 网上银行系统信息安全通用规范

JR/T 0171—2020 个人金融信息保护技术规范

ISO 21586—2020 Reference data for financial services - Specification for the description of banking products or services (BPoS)

3 术语和定义

下列术语和定义适用于本文件。

3.1

银行客户 bank’s customer

在银行经营的全生命周期中，已经或可能与银行发生业务关系的当事人。

注：当事人可能是自然人，也可能是法律认可的组织。

[来源：GB/T 31186.1—2014，3.1]

3.2

个人客户 personal customer

指作为银行客户（3.1）的自然人。

[来源：GB/T 31186.1—2014，3.2]

3.3

网上银行 internet banking

银行业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，包括个人网上银行和企业网上银行等服务渠道。

注：服务渠道包括：

——网站服务；

——App 服务；

——公众号服务；

——小程序服务；

——开放银行服务。

[来源：JR/T 0068—2020，3.1，有修改]

3.4

用户 user

与网上银行（3.3）交互的个人客户（3.2）。

[来源：GB/T 25000.10—2016，3.6，有修改]

3.5

使用质量 quality in use

指定用户（3.4）使用网上银行（3.3）满足其要求的程度，以达到在指定的使用周境中的有效性、效率和满意度等指定目标。

注：在银行内部的网上银行相关工作中，往往将使用质量与“用户体验”一词关联。

[来源：GB/T 25000.10—2016，3.15，有修改]

3.6

可用性 availability

可用性表示当需要使用时，应用系统或部件可操作和可访问的程度。在本文件中，可用性指应用系统的可用性。

[来源：GB/T 37046—2018，3.7，有修改]

3.7

易用性 usability

在指定的使用周境中，产品或系统在有效性、效率和满意度特性方面为了指定的目标可为指定用户使用的程度。

注：易用性既可以从它的子特性角度当作产品质量特性来进行指定或测量，也可以直接通过测度（使用质量的子集）来进行指定或测量。

[来源：GB/T 25000.10—2016，4.3.2.4]

3.8

创新 innovation

新的或被改变的实体，以实现或重新分配价值。

注1：新颖性和价值是相对于且取决于组织和相关利益方的感知。

注2：创新可以是产品、服务、流程、模型、方法等。

注3：创新是一种结果。“创新”这个词有时指旨在或导致创新的活动或过程。当“创新”在这个意义上使用时，它应该与某种形式的修饰语一起使用，例如“创新活动”。

[来源：ISO 56000:2020，3.1.1]

4 缩略语

下列缩略语表示适用于本文件：

API：应用程序编程接口（Application Programming Interface）

App：客户端应用软件（Application Software）

SDK：软件开发工具包（Software Development Kit）

H5：超文本5.0（HTML 5.0）

IP：互联网协议（Internet Protocol）

PC：个人电脑（Personal Computer）

5 基本原则

银行业金融机构的网上银行宜遵循合规性、安全性、易用性、创新性的原则建设和提供服务。

——合规性。即遵循国家相关法律和金融监管机构许可的范围及规定提供服务。

——安全性。即通过服务设计、业务和技术等方式，实现对客户资金安全、信息安全、隐私安全和知情权的有效保障。

——易用性。即通过合理的流程设计、界面交互设计，进行信息无障碍暨适老化改造，弥合数字鸿沟，为不同年龄、区域、操作能力的群体提供可适配的网上银行服务。

——创新性。即通过持续地组合运用技术迭代、功能升级、产品创新的方式优化金融服务，提升客户服务体验。

6 服务形态

6.1 网上银行PC客户端服务

基于个人计算机、键盘、鼠标等硬件终端及该终端上的计算机系统、程序，以IP地址访问或链接银行特定金融应用的网上服务方式。

6.2 手机银行App客户端服务

基于手机、平板电脑等移动设备及该设备预置的相关操作系统，实现无线访问金融类移动应用程序（App）的银行服务方式。

6.3 开放银行API服务

基于互联网数字化平台，以API（应用程序接口）、SDK(软件开发工具包）等技术开放的方式，银行机构按照监管许可的业务范围提供的特定金融服务方式。

6.4 场景金融服务

基于API、SDK、H5、小程序等连接方式，通过输出金融产品、服务或引入第三方产品、服务，实现银行产品功能的金融服务方式。

7 服务功能

7.1 金融服务

7.1.1 个人金融服务

7.1.1.1 概述

个人金融服务功能要求如下：

a) 能为个人客户提供多渠道、多功能、多形态、高质量的金融服务，随时、随地满足客户差异化、多元化的需求；
b) 基础服务应能提供：
   1) 账户服务；
   2) 结算服务；
   3) 存款服务；
   4) 安全管理服务；
   5) 客户信息服务；
   6) 其他辅助服务功能。
c) 增强服务宜能提供：
   1) 贷款服务；
   2) 投资理财服务；
   3) 信用卡服务；
   4) 面向专属客群提供专属产品与差异化服务；
   5) 支持根据客户需求和市场情况灵活调整提供的功能、产品与服务。

7.1.1.2 个人账户服务

个人账户服务应能提供账户信息查询服务、账户管理等子服务，其功能要求如下：

a) 账户信息查询服务包括账户一览、资产负债总览、余额查询、当天或历史交易明细；
b) 账户信息查询服务宜包括账户开户网点查询、工资单明细查询；
c) 账户管理服务包括账户添加或删除、账户挂失、账户密码修改及重置、账户销户、账户个性化别名维护等，宜支持账户解挂、账户销户、借记卡与II、III类账户在线申请。

7.1.1.3 个人结算服务

个人结算服务应能提供转账汇款、生活缴费、电子支付等子服务，其功能要求如下：

a) 转账汇款提供行内转账、境内汇款、跨行汇款、手机号转账、汇款明细查询功能，支持不同类型账户之间的转账汇款等功能；

b） 电子支付提供覆盖线上线下多支付场景、支持多种认证手段的电子支付产品，提供第三方快捷支付的签约与解约、支付限额管理、支付明细查询等功能，宜支持多种支付方式的灵活选择；
c） 生活缴费提供缴费项目查询、主动缴费、委托代扣、缴费明细查询等功能，宜支持覆盖全国不同场景的缴费服务；
d） 转账汇款宜提供跨境汇款功能。

7.1.1.4 个人存款服务

个人存款服务应能提供活期存款、通知存款、定期存款、大额存单及存款增值服务等子项，其功能要求如下：

a） 满足不同客户的资金管理使用需求，提供多种存款产品；
b） 提供灵活的存款计息方式。

7.1.1.5 个人贷款服务

个人贷款服务宜提供信用贷款、质押贷款、抵押贷款、住房贷款、经营贷款等子服务，其功能要求如下：

a） 宜提供在线贷款申请、在线调额、贷款信息查询、还款明细查询、联系方式维护、贷款试算、申请进度查询、自助还款、房贷报税查询及其他功能；
b） 个人信用贷款宜支持无担保、无抵押的授信方式，支持纯线上办理，实时到账，随借随还，循环使用；
c） 抵押贷款宜支持办理抵押登记的不动产为担保贷款提供服务；支持自助提款，贷款额度灵活，贷款期限自由，贷款资金循环使用随借随还；
d） 住房贷款宜支持一手住房购置贷款、二手住房购置贷款、公积金委托贷款、组合贷款的网上申请；
e） 经营贷款宜支持面向小微企业主和个体工商户、农户提供用于生产经营的贷款服务，支持线上办理，押品在线评估，业务智能化审批，自助提款、还款，额度循环使用。

7.1.1.6 个人投资理财

个人投资理财宜提供理财、基金、债券、贵金属、账户交易、外汇买卖及其他子服务，其功能要求如下：

a） 理财宜提供理财产品购买与赎回、预约与撤单、产品查询、持仓查询及其他服务；
b） 基金宜提供基金买卖、交易明细查询、基金交易账户管理及其他功能；
c） 债券宜提供柜台记账式债券和储蓄国债业务的网上交易、持仓查询、明细查询、账户管理、行情查询、记账式债券走势图查询等功能；
d） 贵金属宜提供积存贵金属和品牌贵金属等功能；
e） 账户交易宜提供账户贵金属、账户外汇、账户能源、账户基本金属、账户农产品的网上交易、持仓查询、明细查询、行情查询、保证金管理等功能；
f） 结售汇宜提供人民币与外币的兑换功能；
g） 外汇买卖宜提供多个币种间的外汇买卖功能，以及外汇持仓查询、明细查询、账户管理、挂单管理、保证金管理及其他功能。

7.1.2 对公金融服务

7.1.2.1 概述

对公金融服务功能要求如下：

a) 能为对公客户提供多渠道、多功能、多形态、高质量的金融服务，随时、随地满足客户差异化、多元化的需求。

b) 基础服务应提供：

1） 账户服务；

2） 资金结算服务；

3） 存款服务；

4） 贷款服务；

5） 其他辅助服务功能。

c) 增强服务宜提供：

1） 投资理财服务；

2） 金融市场服务；

3） 现金管理服务；

4） 资产托管服务；

5） 国际结算服务；

6） 票据服务；

7） 面向专属客群提供专属产品与差异化服务；

8） 提供根据银行业务情况、客户需求和市场情况灵活调整的功能、产品与服务。

7.1.2.2 对公账户服务

对公账户服务应能提供账户信息查询、账户管理、数字函证等子服务，其功能要求如下：

a) 账户信息查询服务包括账户一览、余额查询、当天或历史交易明细、账户开户网点查询、电子回单、电子对账单等功能；

b) 账户管理服务支持通过企业手机银行线上预约开立对公结算账户；

c) 宜提供数字函证服务，支持企业客户通过网上银行发起、接收数字函证，并异步完成数字函证业务授权确认、协议签订、进度查询、明细查询业务。

7.1.2.3 对公资金结算服务

对公资金结算服务应提供转账汇款、在线缴费、代理结算、收款及其他收付款子服务，其功能要求如下：

a) 转账汇款支持逐笔或批量方式向全国范围内各家银行的企业和个人账户办理转账汇款。宜提供批量文件制作工具软件，离线制作编辑批量支付指令，批量处理付款业务；

b) 资金结算服务宜支持结合客户需要灵活配置权限组合和授权管理，满足企业内部管理要求；

c) 收款业务宜支持收款企业通过企业网上银行主动扣取经过授权签约的企业或个人客户的各类应缴资金，宜支持批量指令的汇总记账；

d) 代理结算宜支持为中小金融机构提供代理人民币转账、代理外汇汇款、代理本票、代理汇票等服务。

7.1.2.4 对公存款服务

对公存款服务应能提供活期存款、通知存款、定期存款、协定存款、协议存款、大额存单等子服务，其功能要求如下：

a） 应区分不同客户资金管理使用需求，提供不同类型的存款产品；

b） 应提供定期存款和通知存款服务，支持线上开立、提前支取、到期支取、逾期支取、账户信息查询和操作指令查询；

c） 宜提供网上办理协定存款和协议存款服务，支持客户在线通过指定结算账户办理协定存款和协议存款业务。

7.1.2.5 对公贷款服务

对公贷款服务应能提供贸易融资、信用贷款、质押贷款、其他融资子服务，其功能要求如下：

a） 贷款服务支持通过网上银行办理信贷业务的申请、提款、还贷，并可查询各种贷款的合同、借据等信息；

b） 贷款服务支持企业查询贷款的借款、放款、归还、借据等各类信息，随时掌握企业的资金和财务状况；

c） 贷款服务宜区分不同层级客户需要，为大型集团客户提供网络循环贷款、业务不落地、额度循环使用等功能，为中型客户提供抵押贷款、供应链融资服务，为小微客户提供线上小额信用贷款服务。

7.1.3 普惠金融服务

普惠金融服务功能要求如下：

a） 基础服务应能为中小微企业和个体工商户提供：

1） 线上预约开户服务；

2） 结算服务；

3） 融资服务，包括向小微客户在线提供小额信用贷款服务。

b） 增强服务宜提供：

1） 支持企业主个人账户与企业账户的统一管理；

2） 为小微企业提供场景化线上融资，实现特定场景下的预授信和线上放款；

3） 基于担保方式不同，提供信用、质押、抵押等差异化的贷款服务，支持“线上申请、自动审批、随借随还”，提高小微企业贷款服务效率；

4） 提供丰富的企业综合服务，包括工商注册、税务代办、组织机构代码证代办、账户开立、结算服务及其他服务；

5） 提供数字信用凭据融资产品，服务产业链上下游小微客户群。

7.2 非金融服务

7.2.1 概述

非金融服务是基于网上银行系统满足客户需求提供的非金融类延伸服务，包括信息服务、积分商城和其他网络数字子服务。

7.2.2 信息应用服务

信息应用服务功能要求如下：

a） 基础信息服务应提供：

1） 建立全行场景服务和信息服务平台，开展第三方场景和信息服务合作，形成综合场景信息服务生态圈；
2） 场景化、智能化的轻金融服务嵌入式场景和信息服务。

b） 增强信息服务宜提供：
1） 提供银行支付、生活缴费、交通出行等民生、政务类与人们生活密切相关、客户需求量大的场景和信息服务；
2） 根据场景和信息服务合作主体、面向用户范围、主要功能等差异，提供分级分类信息服务与管理；
3） 对场景服务提供主体进行身份信息认证、对信息内容进行检测审核，保证服务提供真实可靠、合法合规。

7.2.3 积分商城服务

积分商城服务功能要求如下：

a） 基础服务应提供：
1） 建立全行客户权益运营服务平台，开展第三方电子商城合作，提供基于本行客户权益的商品、商务服务；
2） 提供积分兑换、福利采购及其他服务。

b） 增强服务宜提供：
1） 面向不同客户群体提供特色服务，为个人客户提供积分抵现、消费信贷、消费分期付款等特色服务，为公司、机构、金融同业等对公客户提供信息展示、线上支付、撮合报价、网络询价、网络竞拍、资产处置、差旅报销、福利采购、网络融资等特色商业或金融增值服务，为信用卡客户提供集生活、消费、金融于一体并整合支付、融资、生活消费场景的综合化服务；
2） 提供乡村振兴特色服务，为助农商户提供服务费、保证金减免优惠政策及快速上线服务，设立助农专区以支持县域企业和个人在线销售农产品；
3） 建设企业商城，为个人客户和对公客户提供境内商品交易、跨境商品交易、金融产品交易、在线支付、在线融资等服务。

7.2.4 音、视频（直播）服务

音、视频（直播）服务功能要求如下：

a） 基础服务应提供：
1） 建立音、视频（直播）运营服务平台，实现远程、异地、专属人员基于 5G 技术开展视频录播、互动直播、视频宣传、业务受理等服务；
2） 开展第三方平台场景合作，提供可视化数字金融服务。

b） 增强服务宜能提供：
1） 提供视频、音频、图文等多种形式的资讯内容服务，为客户提供投资引导、金融知识普及、产品介绍、生活资讯等多元化视频内容服务；
2） 提供直播销售服务，基于消费市场新业态、新模式，提供直播产品展示、发言互动、推广销售及线上购买等服务；
3） 提供客户经理远程音视频业务受理，为客户提供产品介绍、业务问题处理、业务推介、投诉建议等服务。

8 服务体验

8.1 界面设计

网上银行客户端界面设计应本着以用户为中心、便捷、美观、容错、易学、易操作的基本原则开展，功能设计要求如下：

a) 移动端界面设计应符合 T/NIFA 13—2022 中的相关要求；
b) 桌面端界面设计应符合 T/NIFA 14—2022 中的相关要求；
c) 开屏广告时间应控制在 5 秒以内。

8.2 信息无障碍服务

面向个人用户的页面，应符合GB/T 37668—2019、GB/T 41391—2022中的相关要求。其中移动金融客户端页面应符合《移动金融客户端应用软件无障碍服务建设方案》（银发〔2021〕69号）中的相关要求。

8.3 自动化决策服务

网上银行所提供的自动化决策服务，包括向客户进行个性化信息推送或产品营销、开展客户画像等内容，功能要求如下：

a) 提供自动化决策服务时，应当保护客户合法权益，不得根据客户的偏好、交易习惯等特征，利用自动化决策在交易条件上实行不合理的差别待遇等违法行为，强制或者变相强制客户接受金融产品或者服务，或者排除、限制客户接受同业机构提供的金融产品或者服务；
b) 开展客户画像服务时，应符合个人信息保护、消费者权益保护、互联网信息服务算法等法律法规的规定，确保客户画像依据来源合法，尊重客户人格尊严，避免使用有违社会公德、歧视性、偏见性用户标签，发现客户画像存在错误的，应及时进行修改；
c) 应规范信息内容管理，建立用于识别违法和不良信息的特征库，完善入库标准、规则和程序；
d) 应规范用户模型和用户标签管理，完善记入用户模型的兴趣点规则，不得将违法和不良信息关键词记入用户兴趣点或作为用户标签并据以推送信息内容，不应对客户拒绝个性化信息推送或产品营销设置障碍、收取费用或设定有效期限；
e) 应杜绝提供针对其个人特征的选项，应向客户提供便捷的关闭自动化推荐服务的选项，用户选择关闭自动化推荐服务的，页面选项应提供停止服务的按钮。

8.4 权益保护

网上银行应提供对产品服务的信息知情权、资金交易安全权、服务自主选择权、自动化推荐公平交易权、以及在线客服沟通反馈机制保障。

a) 保障客户的银行产品和服务知情权，按照 GB/T 32319 和 ISO 21586 的相关要求向客户进行说明，其内容要求如下：
   1） 客户对该金融产品或者服务的权利和义务，订立、变更、中止和解除合同的方式及限制；
   2） 银行对该金融产品或服务的权利、义务及法律责任；
   3） 贷款产品的年化利率；
   4） 客户应当负担的费用及违约金，包括金额的确定方式，交易时间和交易方式；
   5） 因金融产品或者服务产生纠纷的处理及投诉途径；

6） 对该金融产品或者服务所执行的强制性标准、推荐性标准、团体标准或者企业标准的编号和名称；
7） 在金融产品说明书或者服务协议中，实际承担合同义务的经营主体完整的中文名称；
8） 其他可能影响金融消费者决策的信息。

b) 保障客户资金交易安全权，建立全流程管控机制，在金融产品或者服务的设计开发、营销推介及售后管理等各个业务环节的要求如下：
1） 按照审慎原则，采用电子签名、数字证书等方式，保证客户身份认证、支付交易敏感信息核验和资金交易数据的机密信和完整性；
2） 根据金融产品或者服务的特性评估其对客户的适合度，合理划分金融产品和服务风险等级以及客户风险承受等级，将合适的金融产品或服务销售给适当的客户；
3） 建立交易过程的数据监测、分析、干预机制，防范潜在的非法交易和欺诈交易，通过交易确认、交易提醒、限额设定等方式有效管控交易风险；
4） 为客户提供自助设立交易安全锁、支付限额、一键退出等安全功能。

c) 保障客户服务自主选择权，要求如下：
1） 应采用显著、清晰的方式标识利率、费用、收益及风险等与金融消费者切身利益相关的重要信息，应当根据金融产品或者服务的复杂程度及风险等级，对其中关键的专业术语进行解释说明，并以适当方提供给客户，确认其已接收完整信息；
2） 应当尊重客户购买金融产品或服务的真实意愿，不得违规代理客户办理业务，不得擅自修改客户的业务指令，不得强制搭售其他产品或服务。

d) 保障客户诉求能得到及时、有效的响应，服务要求如下：
1） 设立专门的渠道为客户提供咨询服务和投诉受理，形式包括端内智能客服、电话客服、智能客服在线转换人工客服及其他，及时处理诉求；
2） 通过电话接收处理的投诉应符合 GB/T 32315—2015 关于投诉处理的相关要求，端内人工客服应参照该要求处理；
3） 建立对特殊客户群体的绿色响应机制，提供对残疾人、老人、未成年人等弱势群体客户身份认证、大额异常交易、账户资金继承等特定场景服务。

9 服务安全

9.1 注册和身份认证

本项服务要求如下：

a) 为客户注册并开通网上银行服务应审核客户身份，按照客户申请的事项为其办理相应业务，并保存客户的申请记录；
b) 为客户提供网上银行服务前，应与客户明确相关权利义务和业务办理规则，约定责任承担方式，并保存客户签订的协议文本；
c) 银行人员应依据申请资料、业务凭证和服务协议进行系统操作。对于风险等级较高的业务，操作人员的系统操作应经审核授权后才能生效，作为操作依据或操作结果的业务凭证应按相关规定保管；
d) 为客户开通网上银行服务，应为客户发放安全认证工具或开通安全认证方式，包括但不限于 U 盾、电子密码器、短信认证、生物特征及其他，严禁任何人员骗取或截留客户安全认证工具、套取或窥探客户密码；

e） 对于未成年人、老年群体和残疾人等特殊群体，应制定相应的服务流程提供安全的注册和身份认证服务；

f） 宜建立网上银行系统间统一的用户体系，设计安全的用户身份信息识别机制，用户注册、登录信息核验管理应纳入后台风险监控系统处理，为网上银行业务安全防护提供有力支撑。

9.2 交易验证和限额控制

本项服务要求如下：

a） 应建立交易全流程的安全隐患分析机制，通过交易确认、交易提醒、限额设定等控制策略，有效防范交易风险；

b） 应建立由交易认证、限额控制、风险监控构成的多层次、立体化安全防护体系，根据交易风险级别的不同，设置差异化的业务安全防护策略，保障客户网上银行交易安全；

c） 应提供灵活的安全认证组合服务，根据交易风险级别，采取相应的安全认证方式验证客户身份及交易真实性，在大额转账场景中为客户提供U盾、电子密码器等由独立硬件设备承载的安全认证介质，确保客户交易安全；在小额支付缴费场景中为客户提供基于短信认证、静态密码、生物识别等无介质安全认证方式，提升客户交易便利性；

d） 应根据安全认证工具或安全认证方式的安全性和可靠性，设置合理的交易限额；

e） 应通过事中风险监控对高风险交易进行实时监测，根据交易的可疑程度，采取增强认证、落地处理、拒绝交易等干预措施，保障客户资金安全；

f） 应具备防范客户端数据被篡改的机制，由客户确认资金类交易关键数据；

g） 资金类交易中，如果客户端对交易数据签名，签名数据除流水号、交易金额、转入账号、交易时间等要素外，还应包含由服务器生成的随机数据。对于从网上银行客户端提交的交易数据，服务器应验证签名的有效性，并安全存储签名；

h） 资金类交易中，应对客户端提交的交易信息间的隶属关系进行严格校验，例如验证提交的账号和卡号间的隶属关系以及账号、卡号与登录用户之间的关系；

i） 能够根据客户情况界定高风险业务及其风险控制规则，对于资金类交易等触发风险控制规则的情况，宜使用统一客服号码请求客户反馈确认交易信息；

j） 对于客户资金交易类及其他高风险业务，应通过客户预留的联系方式，提供定向通知方式（手机短信、App、小程序等）及时通知客户资金变化的服务，告知客户其资金变化。

9.3 风险交易识别和监控

本项服务要求如下：

a） 应建立明确的交易风险监控目标，防范网上银行渠道发生的电信诈骗风险、非本人交易风险、洗钱与外汇合规风险、刷单套券风险等；

b） 应建立交易风险监控系统平台，能够对存在资金安全风险或网上银行账户安全风险的交易进行实时风险监控；

c） 宜建立网上银行交易风险监控系统运营队伍，制定网上银行异常交易监测、处理的制度和流程，监测规则、处理机制应能实现：

——交易风险识别。综合运用大数据分析技术等方法，系统而全面地识别出潜在风险点和风险特征；

——交易风险评估。从风险发生的可能性和危害程度确定风险等级；

——交易风险预警。根据风险评估结果，优化、整合和集成“交易->设备->账户->客户”四位一体的风控规则及模型，对交易数据进行实时分析产生风险等级预警信息；

——交易风险控制。根据交易风险等级预警信息，运用针对性措施进行实时干预，实施差异化风险防控，保障客户资金安全。

d）网上银行交易风险监控系统宜能支持通过分析风险事件特征、用户交易习惯和群体用户行为习惯，及时动态创建、更新风险监控模型及规则，提高交易分析的效率和准确率；

e）网上银行交易风险监控系统宜运用人工智能技术开展反欺诈建模，对交易进行欺诈评分，提高欺诈交易的识别能力；

f）应及时收集、统计、核实、分析、处置客户反映的风险事件，并对剩余风险进行再识别、评估、预警及控制，形成交易风险监控闭环。

9.4 新型网络违法犯罪活动防控

本项服务要求如下：

a） 应规范网上银行注册环节的客户身份识别工作，需使用安全认证介质时，应确保介质发放到客户本人；

b） 应依法依规开展客户尽职调查，结合企业和个人客户风险特征、行业或职业特点、客户生命周期以及持有金融资产等情况，合理设置网上银行对外支付限额；

c） 应从交易、设备、账户、客户等维度，分析电信网络新型违法犯罪活动特征，动态优化风控模型和风控规则，有针对地识别和防控涉赌、涉诈交易；

d） 对于客户线上支付业务存在异常情况的，应通过人脸识别、短信提示、密码验证等方式，核实客户身份，进一步提高客户线上支付的安全性；

e） 应建立和完善风险信息库，从监管机构、公安机关获取黑名单等风险信息，对涉赌、涉诈客户的线上交易采取管控措施；

f） 应做好反赌、反诈相关宣传，利用门户网站、App 和微信公众号等渠道推送安全知识广告、竞猜答题、防诈骗风险提示等信息，提高客户涉赌、涉诈风险防范能力。

9.5 洗钱风险管理

本项服务要求如下：

a） 应按照“了解你的客户”的原则，做好客户身份识别工作，通过核对客户身份证明文件、验证客户账户密码、收集并审核相关客户资料等方式，对申请开通网上银行服务的客户开展身份识别，并按规定采集客户信息，留存客户身份证明文件复印件或者影印件等相关资料；

b） 对于客户委托代理人办理业务的，应确认其代理关系的存在,并识别代理人和被代理人身份；

c） 在办理业务中发现异常迹象或先前获得的客户身份资料的真实性、有效性、完整性有疑问的，应当重新识别客户身份；

d） 应提供客户身份证件过期提醒、证件有效期更新、客户身份信息补录等功能，确保留存的客户身份信息真实、准确、有效；

e） 应按照安全、准确、完整、保密的原则，妥善保存客户身份资料和交易记录，确保网上银行的客户身份资料和交易记录在保存期限内能足以重现每项交易；

f） 客户身份资料应自业务关系结束当年或一次性交易记账当年计起至少保存 5 年；交易记录应自交易发生当年计起至少保存 5 年；

g） 应严格按照相关法律法规、监管要求将网上银行服务功能纳入反洗钱系统监测范畴，并做好网上银行大额交易和可疑交易的报告工作；
h） 应结合客户洗钱风险分类结果，采取差异化的控制措施，配套适用强化尽职调查、合理设置网上银行交易限额、限制网上银行交易频率、严格网上银行服务审批手续等措施；
i） 应严格落实联合国、中国政府制定的反洗钱和反恐怖融资管理办法，以及相关洗钱风险管理要求，不得为联合国安理会制裁决议名单、中国政府有权机关公布的恐怖分子名单、以及涉敏业务管理制度禁止建立业务关系或提供服务的实体和个人提供网上银行服务；
j） 应按照产品洗钱风险评估要求，定期对网上银行产品开展洗钱风险评估，结合产品固有风险采取针对性管控措施，防止不法分子利用网上银行开展洗钱或恐怖融资活动。

9.6 客户信息保护

客户信息应按照GB/T 31186给出的模型有序组织。客户信息保护应符合GB/T 35273—2020、GB/T 41391—2022、JR/T 0171—2020的要求，尤其是：

a） 隐私政策链接位置应突出、无遮挡，文本文字显示方式（字号、颜色、行间距）应易于用户阅读；
b） 应明确标识发布、生效或更新日期，并在隐私政策更新时通过弹出提示等方式及时告知用户；
c） 逐项列举 App 各业务功能收集个人信息的情况，并对个人敏感信息类型进行显著标识（如字体加粗、标星号、下划线、斜体、颜色）；
d） 应对个人信息存放地域（国内、国外）、存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行明确说明，将涉及出境的个人信息类型逐项列出并显著标识；
e） 对于涉及将个人信息用于用户画像、个性化展示等应用场景的，应说明可能对用户产生的影响；
f） 对于涉及对外共享、转让、公开披露个人信息的，应明确其目的、涉及的个人信息类型、接收方类型或身份；
g） 对于使用嵌入第三方代码、插件（如 SDK）收集个人信息的，应说明第三方代码、插件的类型或名称，以及收集个人信息的目的、类型、方式；
h） 应对 App 运营者基本情况进行描述，至少包括公司名称、注册地址、联系方式；
i） 应对 App 在个人信息保护方面采取的措施和具备的能力进行说明，如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计；
j） 应明确说明个人信息的查询、更正、删除、用户账户注销、撤回已同意授权的操作方法，并提供电子邮件、电话、在线客服等投诉渠道；
k） 应避免出现免除自身责任、加重用户责任、排除用户主要权利等不合理条款。

10 服务保障

10.1 战略保障

本项要求如下：

a） 宜通过战略指引，构建与数字经济相适应的数字化经营体系，打造开放、合作、共赢的互联网场景生态布局，持续为客户提供便捷安全、高效优质、极致体验的线上金融服务，实现新的价值创造，服务实体经济；
b） 宜通过战略规划，实现金融与科技的融合，促进数字化、智能化、开放化金融服务建设，构建数据驱动和智能服务的服务模式，提升网上银行服务水平；

c） 宜通过战略实施，提升面向小微企业、年轻客群、老年客群、长尾客群和中高端客群的服务供给能力，满足广大客户生产经营和生活消费的金融服务需求；

d） 宜编制网上银行中长期发展规划和短期发展目标，分解落实任务目标，有计划、分步骤地推进战略的落地实施。

10.2 制度保障

本项要求如下：

a） 应建立网上银行业务制度体系，制定网上银行业务管理规定、操作规程和平台服务规则，覆盖网上银行的需求设计、内部控制、合规管理、风险管理、信息安全、业务连续性、数据管理等制度领域和流程环节的管理；

b） 应建立迭代信息安全管理体系，内容包括网上银行平台架构、网络应用、系统设计、编码、测试、集成、运营维护以及评估应急处置等环节；

c） 应建立网上银行平台合作制度，引入具有自主知识产权的技术合作，充分审查、评估合作服务商的经营状况、财务状况和实际风险控制与责任承担能力，进行必要的尽职调查，明确业务合作双方权利、义务关系，严格履行保密义务和保密责任，形成技术专利，进行知识产权保护控制，固化高水平的科技应用成果；

d） 应建立配套的应急处理制度，制定网上银行应急计划和事故处理预案，并定期对这些计划和预案进行测试，以管理、控制和减少意外事件造成的危害。

10.3 组织保障

本项要求如下：

a） 应制定总行层级的互联网金融战略决策机制，审核发展规划和资源配置方案，以及重大网络金融项目决策；

b） 应建立专属部门牵头协同机制，统筹网上银行业务发展与管理，统筹网上银行平台的用户发展与建设运营，统筹网上银行渠道与互联网企业的联动合作；

c） 宜成立专门团队或部门组织开展互联网金融业务系统研发、信息安全、科技管理工作。

10.4 人才保障

本项要求：

a） 宜组建互联网金融专业人才队伍，搭建前瞻性、战略性、系统性人才培训体系，打造一支“懂政策、懂业务、通技术、善经营”的复合型人才队伍，承担网上银行产品研发、业务管理、市场拓展等工作；

b） 宜组建场景运营专业人才队伍，探索数据运营、流量运营、内容运营、客户运营，构建以数字化、智能化为特征的集中统一的线上运营模式；

c） 宜组建用户体验设计的专业人才队伍，开展用户研究、架构设计、流程设计、交互设计、视觉设计、可用性测试、体验设计制度建设、体验设计资源管理及其他体验设计工作；

d） 宜组建软件开发、生产管理和技术保障的专业人才队伍，定期组织技术交流和培训，保障网上银行系统安全运行；

e） 宜组建网上银行服务保障专业人才队伍，配备充足的电话客服，并持续开展培训和服务质量管理，保障网上银行客户服务水平。

11 业务创新

11.1 概述

网上银行业务创新宜遵循“科技向善，智慧为民”的原则，围绕“建设数字中国”战略部署，融合大数据、人工智能、物联网等新技术应用场景，让最新的技术成果在网上银行平台架构上快速部署、融合、应用，带动和促进网上银行多渠道、多模式、多业态、高质量发展，实现金融场景泛在化、融合应用开放化、产品服务智能化。创新策略和方法可参考附录 A。

11.2 特定领域创新

11.2.1 开放化创新

通过开放化创新，宜支持：

a) 建立统一的互联网金融场景化开放平台，将金融科技服务能力开放输出到外部合作方，打通“行内与行外”“金融与非金融”，满足客户多元化一体化金融服务需求；
b) 在开放平台的能力种类上，遵循对外输出账户管理、资金结算及其他金融服务的行业监管规定和市场公平竞争要求，选择商业、服务业、交通等各类生产生活领域，面向民生服务、公共事业、医疗教育、文化娱乐、衣食住行及其他热点行业开展场景共建；
c) 在开放平台的业务流程上，建立“服务开发、服务测试、服务发布、合作方申请、业务准入、接入测试审核、正式上线、运营分析”的统一 API 生命周期管理，为合作方提供便捷的线上对接自助流程；
d) 在开放平台的发布管理上，支持全行产品服务统一发布及管理，建立对外与合作方系统对接的统一接入渠道，为合作方提供查询获取服务信息的通道；
e) 在开放平台的技术架构上，提供高可用、弹性伸缩的技术支持，服务具备弹性伸缩和动态扩容的能力，以支持高业务并发场景；
f) 在开放平台的安全控制上，采用统一身份认证、并发控制、白名单控制、交易防重放、权限控制、数据加密手段，通过建立多维度的监控视图有效应对服务开放可能带来的业务爆发性增长和不可测事件，保证后端产品系统平稳运行；
g) 在开放平台的场景建设上，在场景选择方面优先选取能满足客户拓展潜力大、交易量大的场景；在合作方选择方面力争选取行业领先、综合评价较高的企业，且至少满足具有获客、活客、收益、数据沉淀等一项能力或潜力；
h) 在开放平台的产品设计上，遵循以客户为中心、开放化、通用性、信息共享和安全性等原则，在合规可控的前提下，做好开放平台产品层面的研发与管理工作。

11.2.2 智能化创新

通过智能化服务创新，宜实现：

a) 依托大数据、人工智能、云计算等新技术，构建网上银行智能化服务，提供客户行为画像服务，满足客户个性化的金融管理偏好；
b) 提供个性化推荐服务，根据不同客群提供线上个性化版本、专区服务及精准服务推荐，提供存款、理财、基金、银行卡、贷款、优惠权益等产品服务推荐，实现精准营销及个性化、差异化的千人千面服务，支持客户关闭个性化推荐服务；

c） 提供智能金融产品及服务，提供个人电子钱包开户、智能投顾及 AI 投顾，实现产品快速更新、精准营销；

d） 提供智能语音服务，运用语音语义识别模型及语义规则，支持客户通过语音指令进行功能导航、业务咨询、信息查询、转账汇款等；

e） 提供智能识别服务，依托大数据、人工智能和图像识别技术，在开户、转账等环节支持拍照自动识别并带入相关信息，减少客户的输入；

f） 提供智能安全检测服务，为客户提供账户总览、安全设置、资产配置三重维度一键智能监测，切实保障客户账户和交易安全；

g） 依托人脸识别、声纹识别等生物识别技术，为客户提供手机银行登录、转账汇款、电子商务支付、缴费支付、U 盾额度等关键环节身份认证，支持企业手机银行中小微企业自助开户、法人客户自助启用 U 盾等功能，提升用户体验，防范外部欺诈风险。

附 录 A
（资料性）
创新策略与方法

A.1 创新策略

参照 ISO 56000:2020，网上银行业务的创新宜遵循如下策略：

创新应具有新颖性和价值，且具有必要和充分特征。没有价值表现的改变不是创新。

创新的新颖性程度是相对的，并由用户的感知来决定。

新颖性的程度可以通过一项创新的属性来表达，例如渐进式创新(逐渐变化)或根本性创新(完全新的或显著的变化)。新颖性的程度也与部署的时间有关。随着时间的推移，一种创新可能会在社会中被广泛接受和传播，从新的走向主流，最终成为过时的。过时的创新不是领跑的技术方案。

价值的实现或再分配可以发生在不同的层面，包括个人、组织或社会。价值可以是财务的，也可以是非财务的，例如收入、储蓄、生产力、可持续性、满意度、授权、参与、经验或信任。价值，不论是正面的还是负面的，都是由相关的利益相关方决定的。

一项创新可以有一个或多个属性来描述其创新内容、创新方式和创新原因。一项特定的创新可以用多个属性来描述：

a) 通过属性描述创新了什么，包括创新的对象和创新的程度；
b) 通过属性描述是如何创新的，包括在创新活动中涉及到的相关方，创新环境（例如内部创新、开放创新、合作创新或在生态系统中的创新），创新所需或事实上已具备的资源，例如技术创新或数字创新；
c) 通过属性描述创新的原因，包括在实施创新时所实现的价值类型，与相关方和环境相关的改变或影响的类型。

实施专利是创新的一种典型表现。制定带有专利的企业标准则是对创新应用的固化和承诺。但是，实施专利不一定带来更大的价值。

从提升 GB/T 25000.10—2016 中 4.2 的 5 个属性的视角测量创新效果，往往能给创新带来更大的价值。

A.2 创新与若干活动的关系

改进与创新的关系。创新和改进都实现了价值，都涉及变化，概念部分重叠，但改进仅限于对现有对象的更改。创新则可以包括引入以前不存在的新对象(通常是在不确定性更大的条件下)。最后，使用现有已知的方法和解决方案进行改进通常不会产生创新。

发明与创新的关系。发明具有新颖性。一项发明被限制在它以前从未存在过的意义上是新的，而一项创新可以是任何新的或改变过的对象，例如产品、服务、过程、模型、方法或其组合。一项创新应该实现价值，这是一项发明所不需要的。一项发明可以演变成为一项创新，但一项创新不一定要包含一项发明。

创造力与创新的关系。创造力是构想出一个原始对象的能力，例如一个想法，一个概念或一个问题的解决方案。创造力通常是创新活动、计划和过程的一部分，并支持这些活动。创造力也是支持创新活

动的文化的一个重要特征。然而，要实现创新，创造力是不够的，它必须辅以其他能力和过程，例如验证、开发和部署。

研究和创新的关系。研究是指以获取新知识为主要目的的理论、实验或调查工作。研究可以（但不一定）为创新过程的不同部分提供输入，例如关于趋势、用户行为和新技术的知识。技术研究可以通过技术转让促进创新过程。

开发和创新的关系。开发涉及到将需求转化为实体的具体特征的系统活动，利用从研究和实践经验中获得的现有知识。一般来说，这意味着基于确定的需求，使用操作过程，发展新的或现有的产品、服务、过程、模型、方法等。开发过程可能会导致创新，但通常是针对增量和持续创新进行优化，因此仅限于此，例如逐步扩展现有产品以满足现有用户。通常需要创新过程来补充现有的开发过程，以便向具有明确或未明确需求和期望的新用户引入新的和完全不同的产品。

A.3 创新过程与活动

创新过程通常由一系列以非线性顺序迭代执行的相互关联或相互作用的活动组成，目的是实现创新。这类过程的例子有:识别机会、创建和验证概念、开发和部署解决方案。创新也可能是不明确以创新为目标的活动或过程的结果。创新可以在没有明确和系统的创新过程的情况下实现，例如通过偶然发现或临时活动。

创新过程可以用来形成不同的过程配置，以适应当前特定的创新主动性。创新过程应该是灵活的，能够适应组织寻求实现的创新类型。

创新过程可能是：

完全或部分地在组织内其他已建立的过程中或独立地实施(例如，产品开发过程和销售过程)；

与其他相关的内部或外部流程有关，例如伙伴合作流程、并购流程、合作流程、研发流程及知识产权管理流程；

在组织内部或跨组织执行，涉及不同的利益相关者，例如使用开放创新、协作创新、价值网络或生态系统。

创新过程是探索过程，其特征是搜索、试验、容忍失败和学习。

创新过程的设计通常是为了识别和测试新环境中的不确定性,在这种新环境中,决策需要基于假设,而不是基于经过验证的知识和事实。不确定性可能存在于不同的领域，这取决于创新的类型，例如市场、监管、技术、组织或资源的不确定性。

因此，创新过程涉及冒险和停止主动行动。并非所有的想法、概念或解决方案都将或必须导致创新。中断或改变的创新计划是创新过程的组成部分，是作为新过程迭代和未来创新努力输入的学习来源。

承担风险的可接受程度取决于组织的创新雄心和创新类型。例如，激进的和颠覆性的创新通常涉及更高的风险。与创新相关的风险承担可以通过以下方式进行管理，例如，从投资组合的角度，将具有不同风险水平的计划纳入其中。与创新活动相关的失败和风险容忍度依赖于组织文化。

参 考 文 献

[1] GB/T 29799—2013 网页内容可访问性指南
[2] GB/T 36651—2018 信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架
[3] GB/T 37046—2018 灾难恢复服务能力评估准则
[4] ISO 56000:2020 Innovation management — Fundamentals and vocabulary
[5] 《移动金融客户端应用软件无障碍服务建设方案》（银发〔2021〕69号）