ICS 03.060
CCS A11

团　体　标　准

T/CBA 209—2021

多智能终端互动的服务渠道模式指南

Guidance for the mode of service channel by using multiple intelligent terminals

2021－06－08 发布　　2021－06－08 实施

中国银行业协会　　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》的规定起草。

本文件由中国银行业协会银行业产品和服务标准化专业委员会提出并归口。

本文件起草单位：中国银行业协会、中国农业银行股份有限公司、中国工商银行股份有限公司、上海浦东发展银行股份有限公司、中信银行股份有限公司。

本文件主要起草人：潘光伟、刘峰、高峰、李宽、仲峻锋、王鹏、赵成刚、陈嘉、刘刚、马骏、汪婕、牟天宇、曾海彬、高心怡、史林、李珅尧。

引　言

随着智能手机等移动终端的普及，移动互联网提供的联机交易越来越广泛，人们越来越多地采用手机APP(Application，应用程序)作为与银行的交互渠道来完成某些业务，手机上应用的APP已经成为各种业务办理的交互工具。这些工具在登录确认和交易确认时的安全性直接影响到用户的客户信息和用户资金以及有价可计量物品的安全。

当用户仅使用单一手机完成基于APP的联机交易系统登录或交易操作、操作确认请求以及确认信息的接收时，存在较大的安全隐患。一是单一手机，存在着手机被入侵后，验证码被恶意软件拦截导致资金损失的可能；二是若单一手机被盗，即便是双卡，也存在着密码重置的验证码发送到同一物理设备的从而难以避免风险的可能；三是在手机给孩子使用时，发生孩子未经允许使用支付功能而家长无法及时控制的风险。

进一步看，目前银行的服务，已经由单纯为客户服务发展到了供应链金融服务的阶段。实际上，供应链不仅仅体现在对公业务中的上下游和供产销关系中，在家庭关系和工作关系里面，只要涉及到金融往来的，都可能存在供应链，例如父母提供资金供孩子上学，子女通过提供资金的方式赡养老人等，都是家庭中的供应链；而单位中，资金支付的批准，同样也可以看做供应链。这些供应链之间的资金关系，往往也是通过手机等设备操作的。因此，通过某种方式能够使得这样供应链资金转移能做到安全和透明，也有着迫切的需求。

本文件即在考虑上述情况的基础上，给出了多终端互动的服务渠道模式指南，通过多终端的协作以及多终端间的安全通信，共同构建了统筹考虑灵活和安全的银行产品服务支付渠道，并可构建由客户参与管理的可信供应链支付，以供银行业金融机构能向具备条件的客户提供更好的服务。

在按照GB/T 32319-2015、ISO 21586:2020向客户提供银行产品服务的说明书，或按照T/CBA 207-2020向银行员工提供关于银行产品服务手册时，本文件能够成为说明销售渠道和服务渠道的直接引用的文件或参考文献。

本文件的发布机构提请注意，声明符合本文件时，本文件的第6章可能涉及已授权专利201510578574.1《一种利用多移动终端进行联机交易的处理方法》的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：中国农业银行股份有限公司

地址：北京东城区建国门内大街69号

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

多智能终端互动的服务渠道模式指南

1 范围

本文件给出了多智能终端互动的服务渠道模式的系统框架，描述了适合的银行产品服务(BPoS)，提供了此模式的特定业务过程的指南。

本文件适用于中国银行业协会会员单位作为银行产品服务提供商(BPoSP)向其客户提供BPoS时参考。

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 32319—2015 银行业产品说明书描述规范

JR/T 0068—2020 网上银行系统信息安全通用规范

ISO 21586:2020 金融服务参考数据 银行产品服务（BPoS）描述规范（Reference data for financial services — Specification for the description of banking products or services (BPoS)）

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本文件。

3.1

银行产品 banking product

BPoSP（3.4）的输出，可以在BPoSP与客户（3.5）之间不进行任何交易的情况下进行生产。

注：在根据ISO 9000定义银行产品的情况下，该术语可能等于BPoS。

[来源：ISO 21586:2020,3.1]

3.2

银行服务 banking service

BPoSP（3.4）的输出，在BPoSP和客户（3.5）之间至少需要执行一个活动。

注：在根据ISO 9000定义银行服务的情况下，该术语可能等于BPoS。

[来源：ISO 21586:2020,3.2]

3.3

银行产品服务 banking product or service

BPoS

供应商为满足客户的金融需求或与金融相关的需求而向客户(3.5)提供的输出。

注 1：BPoS 的范围是 CPC 版本 2.1 中 group 711 的一个子集，即包括一些金融服务，但投资银行、保险服务和养老服务除外。

注 2：客户可以将 BPoS 作为产品或服务，或者作为产品和服务不可分割地交织在一起。另见 CPC 版本 2.1 第二章“分类的基本原则”C.“商品、服务和其他产品”。

注 3：如果提到了 BPoS 的复数形式，例如一族 BPoS 或一组 BPoS，则缩略语仍然是 BPoS。

［来源：ISO 21586:2020,3.3］

3.4

银行产品服务提供商 banking product or service provider

BPoSP

向客户(3.5)提供BPoS(3.3)的组织。

注：BPoSP被认为是直接向客户交付BPoS的组织。

［来源：ISO 21586:2020,3.4］

示例：商业银行是典型的 BPoSP。

3.5

客户 customer

期望获得，或已经获得某BPoS(3.3)（即银行产品或银行服务）的个人或组织。

注：消费者、客户、最终用户、零售商、一个内部过程的产品或服务接受、受益人或购买者均是同义词。

［来源：ISO 21586:2020,3.5］

3.6

智能终端 intelligent terminal

一种有内置的数据处理能力的用户终端。

［来源：GB/T 5271.1—2000，01.03.14］

3.7

移动终端 mobile terminal

区别于PC机方式，以手机、平板电脑、可穿戴设备等访问网上银行的移动设备。

［来源：JR/T 0068—2020，3.5］

注：在本文件中，主要使用智能终端一词，移动终端实际上是智能终端的一种。

3.8

客户端程序 client program

为网上银行客户提供人机交互功能的程序，以及提供必需功能的组件。

注：包括但不限于可执行文件、控件、静态链接库、动态链接库等。本文件中客户端程序包括运行于移动终端上的应用软件，不包括IE等通用浏览器。

［来源：JR/T 0068—2020，3.6，有修改］

3.9

供应链 supply chain

涉及通过上下游联系，向最终客户以产品和服务的方式提供价值的过程和活动的组织网络。

［来源：GB/T 38299-2019，3.6，有修改］

注：本文件中的上下游联系，不仅涉及到组织机构间，还涉及到组织机构内和家庭以及财产共有人之间。

3.10

认证 certification

为实体建立公钥证书的过程。

［来源：GB/T 27928.1-2011，3.13］

3.11

末端证书 end certificate

证书链中最末的证书。

［来源：GB/T 27928.1-2011，3.32］

3.12

认证机构 certification authority

CA

一个或多个实体所信任的实体，它产生、分配、撤销或挂起公钥证书。

[来源：GB/T 27928.1-2011，3.14]

3.13

注册机构 registration authority

RA

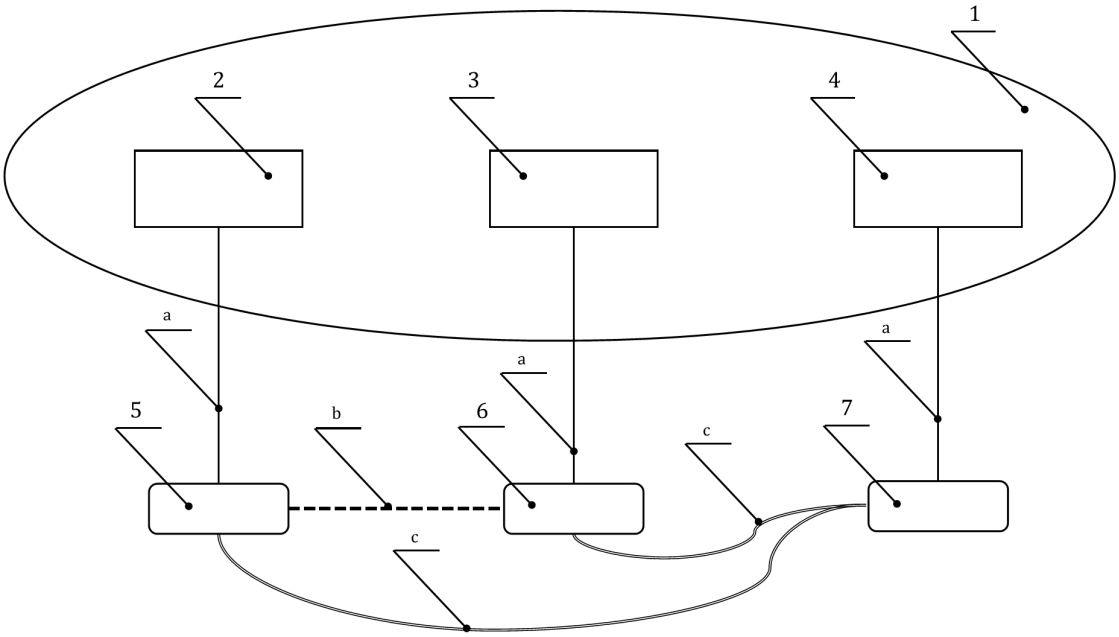
负责证书主体的身份验证和认证的实体，但并非CA，因此并不签名或签发证书。

注：一个 RA 可在证书应用流程、撤销流程或在两者中同时提供协助。

[来源：GB/T 27928.1-2011，3.53]

4 系统框架

多智能终端互动的服务渠道模式逻辑框架如图1所示。



标引序号说明：

1—银行产品服务供应商端的应用系统；

2—智能终端接口服务器A；

3—智能终端接口服务器B；

4—智能终端接口服务器C；

5—智能终端A；

6—智能终端B；

7—智能终端C。

各智能终端接口服务器均是银行产品服务供应商端的应用系统的组成部分，其之间准许执行必要的信息交互，且其之间的交互认为是安全的；根据不同应用系统的设计情况，各智能终端接口服务器在物理上准许是一台服务器。

注 1：银行产品服务供应商端的应用系统仅列出了与多智能终端互动的服务相关的部分。

注 2：从智能终端的视角看，通过智能终端接口服务器与整个银行产品服务供应商的应用系统完成所有需要的信息交互。

[a] 智能终端与智能终端接口服务器之间的通信信道，该信道可能是安全的，也可能是不安全的。

[b] 智能终端之间的通信信道，该信道可能是机读的，也可能是人工视读的。

[c] 智能终端之间的通信信道，该信道是安全的。

图 1　多智能终端互动的服务渠道模式逻辑框架图

5　适合的银行产品服务(BPoS)

本文件描述的多智能终端互动的销售渠道和 / 或服务渠道模式,适合于在BPoS的运作过程中能够准确标识并记录两部及以上智能终端的BPoS。

按照GB/T 32319—2015中6.17或ISO 21586:2020 中6.2.4.2所描述的适合客户，支持包括有如下特征的BPoS。

a) 同一客户具有两部及以上的智能终端，并可用于 GB/T 32319—2015 中 6.25 所描述的销售渠道和 6.26 所描述的服务渠道，或 ISO 21586:2020 中 6.2.4.6 所描述的销售渠道和 6.2.4.7 所描述的服务渠道。

b) 多于一个客户持有不同智能终端，并可用于 GB/T 32319—2015 中 6.25 所描述的销售渠道和 6.26 所描述的服务渠道，或 ISO 21586:2020 中 6.2.4.6 所描述的销售渠道和 6.2.4.7 所描述的服务渠道。

c) 在 GB/T 32319—2015 中 6.30 产品用途和 / 或 6.31 运作原理和流程的描述中，或 ISO 21586:2020 中 6.2.4.10 产品用途和 / 或 6.2.4.11 运作原理和流程的描述中，提及了由两个以上不同个人通过智能终端办理业务的情形。

d) 同时支持 a)、b)和 c)。

6　特定业务过程

6.1　概述

本章仅描述智能终端作为服务渠道应用时,多智能终端互动的服务渠道模式所涉及的特定条件和交互，BPoS的其他属性并未提及。但在设计和实现BPoS时，宜考虑本文件所提出模式给BPoS的其他维度所带来的影响。

示例：只能为有两部智能手机的同一客户，或两个拥有智能手机的干系人提供服务，就是一种本文件描述的服务方式对 BPoS 的影响。

6.2　单专用客户端程序模式

6.2.1　模式特征

单专用客户端程序模式的特征如下。

a) 银行产品服务供应商端的应用系统宜能识别和记录同一客户的两个智能终端的标识。

b) 客户的一个智能终端上安装专用的客户端程序。

c) 客户的另一个智能终端上具有通用的客户端程序。

6.2.2　典型交互

单专用客户端程序模式的典型交互如下。

a) 客户在其智能终端 A 上安装专用客户端程序。
b) 客户用其智能终端 B 的标识码注册安装在智能终端 A 上的专用客户端程序。
c) 客户通过其智能终端 A 上安装的专用客户端程序向智能终端接口服务器 A 发起交易请求。
d) 智能终端接口服务器 A 将请求传递给银行产品服务供应商端的应用系统中的相关业务处理单元，然后：
   1) 确认该业务请求在客户正确登陆智能终端 A 上安装的专用客户端程序后不需要再进行鉴权的，由银行产品服务供应商端的应用系统通过智能终端接口服务器 A 直接将交易响应传递给智能终端 A 上安装的专用客户端程序。
   2) 确认该业务请求在客户正确登陆智能终端 A 上安装的专用客户端程序后需要再进行鉴权的，由银行产品服务供应商端的应用系统通过智能终端接口服务器 B 将交易鉴权信息发送给智能终端 A 上安装的非专用客户端程序；客户需在人工读取该鉴权信息后，将相关的鉴权信息输入到智能终端 A 上安装的专用客户端程序中以完成鉴权。

此交互过程下典型示例见本文件附录A。

6.3 双专用客户端程序模式

6.3.1 模式特征

双专用客户端程序模式的特征如下。

a) 银行产品服务供应商端的应用系统宜能识别和记录同一客户的两个智能终端的标识。
b) 当智能终端的标识能够分为设备标识、可拆卸的部件标识和通信信道标识时，宜能分别记录这些标识，且将对这些标识的依赖纳入业务流程。
c) 客户的两个智能终端上均安装专用的客户端程序。

示例：手机号码、手机的 IMEI、手机的 SIM 卡标识、手机的 TF 加密卡标识、安卓 ID、UUID 均是智能终端标识的例子。

6.3.2 典型基本交互

双专用客户端程序模式的典型基本交互如下。

a) 客户通过其智能终端 A 上安装的专用客户端程序登陆，选择所需的业务功能并填写入相关参数后，形成交易请求信息并发送到智能终端接口服务器 A。
b) 智能终端接口服务器 A 在收到智能终端 A 上安装的专用客户端程序发来的请求信息后，由银行产品服务供应商端的应用系统按照预设的业务逻辑进行处理，随后可做如下处理：
   1) 主动经由智能终端接口服务器 B 向智能终端 B 上安装的专用客户端程序发出信息；
   2) 等待智能终端 B 向智能终端接口服务器 B 发送的请求信息，并对仅在智能终端 B 上安装的专用客户端程序发来的信息所发送的相关标识信息与预记载的信息一致时方进行后继业务逻辑，否则或者拒绝该交易，或者按照 BPoS 设定的特定业务逻辑进行处理。
c) 客户按照其智能终端 A 上安装的专用客户端程序的提示，操作智能终端 B 上安装的专用客户端程序，或者直接读取智能终端 B 上安装的专用客户端程序推送过来的验证码以及相关交易信息，或者通过发送请求要求获得验证码以及相关交易信息。
d) 智能终端 B 上安装的专用客户端程序所接受的信息，可能是可人工视读的，也可能是仅能机读的。
e) 对人工视读的信息，客户将所获得的验证码输入到智能终端 A 上安装的专用客户端程序中；对机读的信息，客户操作两个智能终端完成信息传送。

f) 智能终端 A 上安装的专用客户端程序在接收到用户输入的验证码以及相关交易信息之后，或者当具备足够的安全条件时在本地对相关信息进行验证，或者将这些信息送到智能终端接口服务器 A，然后在银行产品服务供应商端的应用系统内进行验证。通过验证的，交易按照既定的业务逻辑执行；未通过验证的，交易失败。

g) 智能终端 B 上安装的专用客户端程序介入交易宜根据 BPoS 的特征决定，并可条件触发。即智能终端 B 上安装的专用客户端程序在交易开始并不参与交易，但在智能终端 A 上安装的专用客户端程序处理业务的过程中，当输入的某个参数达到预设的阈值时，会提示或者在智能终端 B 上安装的专用客户端程序中获取某些信息，或输入某些信息以完成完整的交易过程。

此交互过程下典型示例见本文件B.1。

6.3.3 典型安全交互

双专用客户端程序模式的典型安全交互，在典型的基本交互过程基础上，还宜支持如下功能。

a) 当银行产品服务供应商端的应用系统具有认证中心 CA 或注册审批机构 RA 的能力，而智能终端 A/B 具有安全存储能力时，智能终端 A/B 上安装的专用客户端程序宜通过智能终端接口服务器 A/B 获取数字证书，随后智能终端 A/B 上安装的专用客户端程序与智能终端接口服务器 A/B 的通信均通过所获取的数字证书进行加密和数字签名，其中需要加密和计算摘要的内容，由智能终端 A/B 上安装的专用客户端程序所支持的 BPoS 要求传送数据的业务规则决定，并符合 JR/T 0068—2020 的要求。

b) 当智能终端 A/B 具有可拔插具备安全存储能力的介质物理能力时，可通过插入该介质获得安全存储能力，且在该介质移除后，不宜再能支持该介质插入时具备的安全功能。

c) 当智能终端 A/B 具有可近场连接或通过蓝牙连接具备安全存储能力的介质物理能力时，可通过连接该介质获得安全存储能力，且在与该介质失去连接后，不宜再能支持该介质连接时具备的安全功能。

d) 在智能终端 A 和智能终端 B 均可获得数字证书的情况下，两者通过通过机读的方式交换信息宜根据 BPoS 的需要判断交互信息的安全性，在需要时通过各自拥有的数字证书加密和签名。

此交互过程下典型示例见本文件B.2。

6.4 自助可信交易链管理模式

6.4.1 模式特征

自助可信交易链管理模式的具有如下特征。

a) 需要至少三个智能终端。

b) 智能终端接口服务器 C 具有 CA 或 RA 能力，可由智能终端接口服务器 C 向智能终端接口服务器 A 和智能终端接口服务器 B 发放末端证书。

c) 智能终端 C 上安装的专用客户端程序宜具有数字证书注册审批机构前端的功能，能够由智能终端 C 直接向智能终端 A 和智能终端 B 以及更多的智能终端发放末端证书。

d) 可由客户自行建立一个可信智能终端组，实现对组内智能终端的动态管理。

6.4.2 典型交互

自助可信交易链管理模式的交互主要是认证的如下过程。

a) 在银行产品服务供应商端的应用系统的控制下，宜通过智能终端接口服务器 C 对智能终端接口服务器 A 和智能终端接口服务器 B 进行认证，以使得智能终端接口服务器 A 和智能终端接口服务器 B 之间在需要时可实现安全通信。

b) 智能终端 C 上安装的专用客户端程序宜具有 RA 前端的功能，宜能够：
   1) 在银行产品服务供应商端的应用系统的控制下，通过智能终端接口服务器 C 与智能终端接口服务器 A 和智能终端接口服务器 B 交互，以完成对智能终端 A 和智能终端 B 的认证；
   2) 直接对智能终端 A 和智能终端 B 及其他的智能终端的认证。
c) 智能终端 C 上安装的专用客户端程序宜能在银行产品服务供应商端的应用系统的控制下管理其所颁发的数字证书，发出申请某智能终端的证书作废的请求。

此交互过程下典型示例见本文件附录C。

6.5 供应链协作模式

6.5.1 模式特征

供应链协作模式具有如下特征。

a) 至少有两个存在确定的金融利益关系的客户，每个客户至少持有一个智能终端。
b) 每个单独的客户都可使用单专用客户端程序模式和 / 或双专用客户端程序模式办理非供应链协作模式的金融业务。
c) 可使用自助可信交易链管理模式，且由操作智能终端 C 的客户管理该供应链协作。

6.5.2 典型交互

供应链协作模式的交互过程包括供应链协作的管理和交易过程控制，如下。

a) 在不使用自助可信交易链管理模式时，宜通过特定的 BPoS 规定两个客户间的交互过程。
b) 在使用自助可信交易链管理模式时，宜由智能终端 C 上安装的专用客户端程序向供应链中客户的智能终端颁发数字证书，并在需要时作废数字证书。
c) 客户间的交互可分为：
   1) 智能终端 A 上安装的专用客户端程序独立执行金融交易，智能终端 B 上安装的专用客户端程序自行发起查询相关账户和交易状况；
   2) 智能终端 A 上安装的专用客户端程序在交易满足 BPoS 设定的条件时，自动通过智能终端 B 上安装的专用客户端程序发送通知；
   3) 智能终端 A 上安装的专用客户端程序在交易满足 BPoS 设定的条件时，在交易过程中向智能终端 B 上安装的专用客户端程序发出授权请求，在得到授权后，方能继续交易。
d) 在使用自助可信交易链管理模式时，智能终端 C 上安装的专用客户端程序可根据 BPoS 中给定的用途和基本运作过程，查询其所颁发数字证书的智能终端的交易情况。

此交互过程下典型示例见本文件附录D。

附 录 A
（资料性）
单专用客户端程序模式示例

A.1 以手机短信为非专用客户端

A.1.1 所需设备

客户需要准备两部手机，其中：

a) 一部可以安装手机银行 APP 作为智能终端 A 上安装的专用客户端程序；
b) 一部可以接收短信。

A.1.2 查询通用信息

当客户拟通过手机银行查询可供选择的理财产品时：

a) 通过手机银行输入（包括选择）拟查询的理财产品；
b) 手机银行与其掌银接口服务器交互，发出交易请求；
c) 掌银接口服务器收到请求信息后，通过银行的业务系统进行判定，确定不需要客户登陆掌银，直接通过掌银接口服务器响应相关理财产品的信息。

A.1.3 查询专用信息

当客户拟通过手机银行查询其活期账户余额时：

a) 通过手机银行输入（包括选择）查询请求；
b) 手机银行或在本地判定该交易需要登陆手机银行，或在与其掌银接口服务器交互后，确定需要客户登陆手机银行；
c) 客户在正确完成手机银行登陆后，发出查询交易请求；
d) 掌银接口服务器收到请求信息后，通过银行的业务系统进行判定，确定不需要进一步鉴权信息，通过掌银接口服务器响应相关账户余额的信息。

A.1.4 转账

当客户拟通过手机银行转账时：

a) 通过手机银行输入（包括选择）转账请求；
b) 手机银行或在本地判定该交易需要登陆手机银行，或在与其掌银接口服务器交互后，确定需要客户登陆手机银行；
c) 客户在正确完成手机银行登陆后，发出转账交易请求；
d) 掌银接口服务器收到请求信息后，通过银行的业务系统进行判定，确定需要进一步鉴权信息，向另一部并未安装手机银行的手机发出短信验证码；
e) 客户通过阅读另一部手机上的短信，在手机银行中输入短信验证码，手机银行通过与手机银行掌银接口服务器通信，确认验证码无误后，执行转账并将结果发送到手机银行。

A.1.5 特别提示

尽管此种方式的安全程度高于在同一手机上安装专用客户端程序并接受短信，但依旧存在短信被诈骗拦截、转移接收的风险。

A.2 以手机微信为非专用客户端

A.2.1 所需设备

客户需要准备两部手机，其中：

a) 一部可以安装手机银行 APP 作为智能终端 A 上安装的专用客户端程序；

b) 一部可以安装微信并支持微信公众号。

注：此例仅考虑将公众号作为信息传送的渠道使用，若通过公众号做进一步的开发，则将开发的成果视作专用客户端。

A.2.2 查询专用信息

客户能够通过手机银行或微信公众号查询其活期账户。

a) 若通过手机银行查询，其过程与 A.1.3 相同。

b) 若通过微信查询，则在微信公众号已经完成了相关银行卡的绑定后，可由微信与其接口服务器通信，发出查询请求，且由于微信已经完成了登陆，在确定不需要进一步鉴权信息后，通过微信接口服务器向微信响应相关账户余额的信息。

A.2.3 转账

当客户拟通过手机银行转账时：

a) 通过手机银行输入（包括选择）转账请求；

b) 手机银行或在本地判定该交易需要登陆手机银行，或在与其掌银接口服务器交互后，确定需要客户登陆手机银行；

c) 客户在正确完成手机银行登陆后，发出转账交易请求；

d) 掌银接口服务器收到请求信息后，通过银行的业务系统进行判定，确定需要进一步鉴权信息，向另一部手机上安装的微信公众号发出验证码；

e) 客户通过阅读另一部手机上的公众微信号的验证码，在手机银行中输入该验证码，手机银行通过与手机银行掌银接口服务器通信，确认验证码无误后，执行转账并将结果发送到手机银行。

注：微信验证码可采用字母数字的混合码，比短信验证码有更强的防猜测能力。

附 录 B
（资料性）
双专用客户端程序模式示例

B.1 典型基本交互

B.1.1 所需设备

客户需要准备两部手机可安装APP的智能手机，但不必要求智能手机具备安全存储功能，也不向客户提供可支持安全存储的附加设施。

B.1.2 前期准备

需做的前期准备工作如下：

a) 客户需在银行网点注册其两部手机；
b) 分别下载手机银行 A 和手机银行 B；其中手机银行 A 和手机银行 B 可以均具有完整的手机银行功能，也可分别具有不同的功能；
c) 分别在两部手机上激活手机银行，并将手机电话号码与手机设备通过设备指纹标识进行绑定。激活可在网点进行，也可通过将短信交叉发送到两个手机上进行。

B.1.3 超过阈值的转账

当客户拟通过手机银行转账时：

a) 通过安装在手机 A 上手机银行选择转账，输入转出账户、对方账户和交易金额，按要求输入交易密码；
b) A 手机的手机银行与其掌银接口服务器交互，发出交易请求；
c) A 手机掌银接口服务器收到请求信息后，通过银行产品服务供应商端的应用系统进行判定，确定该笔交易金额超过阈值，然后返回 A 手机的手机银行需查看手机 B 的手机银行应用所给出验证码的信息。
d) 客户可选择是通过手动还是生成一个二维码，然后
    4) 当选择手动时，手工将 B 手机的手机银行给出的验证码输入到 A 手机的手机银行中；
    5) 当选择二维码时，在 B 手机的手机银行中生成一个二维码，然后用 A 手机扫码获得相应验证码。
e) A 手机的手机银行可执行如下动作之一：
    1) 在本地与从其掌银接口服务器获得的验证码进行比对；
    2) 与其掌银接口服务器交互，将验证码送至银行产品服务供应商端的应用系统进行判定。
f) 判定通过后，完成交易；未能通过判定，则交易失败。

B.1.4 功能冻结

当客户认为失去对任一部手机的控制从而需要暂停其办理业务时：

a) 通过安装在另一部手机上手机银行向银行产品服务供应商端的应用系统发出功能冻结申请；
b) 银行产品服务供应商端的应用系统冻结所申请的手机的手机银行的所有功能。

c） 根据 BPoS 的设计，被冻结的手机银行的响应可以是功能被冻结；也可以是显示通信障碍或交易执行中等信息，并要求被手机银行的手机持续保持开机状态。

注：要求手机持续保持开机状态有可能有助于对手机的定位。

B.2 典型安全交互

B.2.1 所需设备

客户需要准备两部手机可安装APP的智能手机，且满足如下条件之一：

a） 智能手机具备安全存储功能；

b） 为智能手机配套了加密 TF 卡；

c） 为智能手机配套了通过蓝牙连接的 USB-KEY。

注：上述三种方式中，智能手机具备安全存储功能安全性最高，但灵活性最差。

B.2.2 前期准备

需做的前期准备工作如下：

a） 客户需在银行网点注册其两部手机；

b） 分别下载手机银行 A 和手机银行 B；其中手机银行 A 和手机银行 B 可以均具有完整的手机银行功能，也可分别具有不同的功能；

c） 分别在本手机上激活手机银行，并将手机电话号码与手机设备指纹标识进行绑定。激活可在网点进行，也可通过将短信交叉发送到两个手机上进行。

B.2.3 超过阈值的转账

当客户拟通过手机银行转账时：

a） 通过安装在手机 A 上手机银行选择转账，输入转出账户、对方账户和交易金额，按要求输入交易密码；

b） A 手机的手机银行与其掌银接口服务器交互，发出交易请求，所有的交易请求均采用数据证书加密和签名；

c） A 手机掌银接口服务器收到请求信息后，通过银行产品服务供应商端的应用系统进行判定，确定该笔交易金额超过阈值，然后返回 A 手机的手机银行需手机 B 的手机银行应用协同的通知。

d） 用户操作手机 B 的手机银行应用，对访问手机的 SE 进行授权。

e） 手机 B 的手机银行应用采用数字证书加密与签名的方式，与 B 手机掌银接口服务器通信，获取交易确认信息。

f） 在客户的两部手机已经建立了蓝牙连接，或两部手机在同一局域网内时，可由两部手机自行通信，且通信的信息采用采用数字证书加密与签名。

g） A 手机的手机银行可执行如下动作之一：

1） 在本地与从其掌银接口服务器获得的确认信息进行比对；

2） 与其掌银接口服务器交互，将确认信息送至银行产品服务供应商端的应用系统进行判定。

h） 判定通过后，完成交易；未能通过判定，则交易失败。

注 1：此种方式，在安全系统未被攻破前，即便手机本身已经被病毒或木马所侵入，所有通信的信息也是安全的。

注 2：针对特定的 BPoS，在具备了此种通信能力的手机上的手机银行是否均采用此种方式，或通过特定的条件触发此种方式，均由 BPoS 的设计与实现确定。

B.3 典型基本交互与典型安全交互的关系

典型基本交互与典型安全交互具有如下的关系：

a) 所有典型基本交互所能够完全的功能，典型安全交互均能实现，且具有更高的安全性，也可能需要更多的计算开销，且有可能增加交易的响应时间。

b) 在具备典型安全交互的环境中，是否所有的交易均采用数字证书加密和签名，取决于相关 BPoS 的设计与实现。在某种灵活的 BPoS 中，有可能是根据客户的需求进行配置的。

附 录 C
（资料性）
自助可信交易链管理模式示例

C.1 所需设备

客户需要准备三部手机可安装APP的智能手机，且满足如下条件之一：

a) 智能手机具备安全存储功能；

b) 为智能手机配套了加密 TF 卡；

c) 为智能手机配套了通过蓝牙连接的 USB-KEY。

注：上述三种方式中，智能手机具备安全存储功能安全性最高，但灵活性最差。

C.2 前期准备

需做的前期准备工作如下：

a) 客户需在银行网点注册其一部手机作为其自助可信交易链管理设备；

b) 下载手机银行 C，其功能为注册本身的其他手机和向这些手机颁发数字证书；

c) 本手机上激活手机银行 C，并将手机电话号码与手机设备指纹标识进行绑定（例如 IMEI 码、安卓 ID 或 UUID）、以及可能使用的附属安全设备（例如蓝牙的 USB-Key）一并绑定。

注：为了确保安全，此项绑定可能要求只能由本人在网点实施。

C.3 向其他手机颁发数字证书

向其他手机颁发数字证书是此模式使用的首个步骤，且在此步骤执行前，不能执行其他的步骤。

a) 在 A、B 手机上分别安装的手机银行；

b) 使用 A、B 手机中安装的手机银行 APP 分别通过手机 C 下载数字证书。

在A、B手机上分别正确获得了数字证书后，其交互过程与本文件B.2的描述相同。特别要注意的是，手机C并不参加正常的交易，因此该手机可以不必随身携带。

C.4 更换智能终端

用户可随时更换新的智能终端，只需：

a) 作废向原智能终端发出的数字证书，且不论此时该智能终端是否受控；

b) 在新的智能终端下载相应客户端程序后，向新的智能终端标识，有可能是一个新的移动电话号码，或一个新的手机发放数字证书。

允许的智能终端种类由BPoS决定。

附 录 D
（资料性）
供应链协作模式示例

D.1 概述

供应链协作模式可为本文件附录A、附录B和附录C描述示例的组合，但至少涉及到两个自然人。

D.2 家庭供应链

D.2.1 交易明细查询

当父亲或母亲作为子女的资金提供者供其在读书时，某BPoS明确可提供双亲之一对子女的账户交易明细进行查询。

D.2.2 交易即时报告

当某BPoS专门针对夫妇推出时，可提供对一个特定的账户双方均有动账交易的权利，且在一方动账时，将通过手机银行通知另一方。

注：已经广泛使用多年的贷记卡的附属卡就具有类似的功能，但只能是附属卡动账时通知主卡持卡人。

D.2.3 交易即时授权

当子女赡养其父母且提供的资金为其主要经济来源时，某BPoS可允许在其父母的账户发生超出预订额度的交易时进行即时授权。

注：该BPoS的客户为子女或子女与父母，且要求父母至少为限制民事行为能力人。

D.3 公司内供应链

公司内的供应链与家庭供应链类似，但各客户之间的关系为公司的同事。支持公司内部供应链的BPoS与支持家庭供应链的BPoS为不同种类的BPoS。

支持自助可信交易链管理模式的BPoS，可支持公司快速变更其有权动账和有权查看交易明细的人员。

D.4 公司间供应链

D.4.1 支付通知

当通过特定的BPoS支付时，每次在支付完成后，均通知该BPoS允许的干系人。尤其是在BPoS支持与商务合同绑定时，不仅能够提示支付的时间与金额，亦可提供所基于合同支付完成的百分比等信息。

D.4.2 主动收款

在绑定商务合同的BPoS支持时，可在特定的商业条件下，由合同中规定的收款方发起主动收款，该收款的支付条件则取决于BPoS。

参 考 文 献

[1] GB/T 5271.1—2000 信息技术 词汇 第1部分:基本术语
[2] GB/T 27928.1-2011 金融业务 证书管理 第1部分：公钥证书
[3] GB/T 38299—2019 公共安全 业务连续性管理体系 供应链连续性指南