ICS 03.060
CCS A 11

T/SZFCC

苏州市金融业商会团体标准

T/SZFCC XXXX—XXXX

数字人民币智能体交易服务规范

Specification for e-CNY agent-based transaction services

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

苏州市金融业商会　　发 布

目　　次

前言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　基本要求 1
5.1　服务原则 2
5.2　参与主体及权责 2
5.3　服务分层框架 3
5.4　分级管控规则 4
5.5　委托代理与风险责任服务规则 4
5.6　跨域数据流转与数据不出域服务规则 5
6　智能体全生命周期管理 5
6.1　智能体注册 5
6.2　智能体评级认证与动态处置 6
7　前置授权服务 6
7.1　用户身份核验服务 6
7.2　支付委托书开立服务 6
7.3　委托书变更、续期、吊销服务 7
7.4　支付令牌签发与生命周期管理服务 7
7.5　授权边界校验服务 7
8　交易场景服务 8
8.1　S1 用户委托自动支付服务 8
8.2　S2 用户确认式智能支付服务 8
8.3　S3 智能体间 API 小额付费服务 8
8.4　S4 数字人民币智能合约条件支付服务 8
9　风险管控专项服务 9
9.1　L3 大额人工审批服务 9
9.2　交易异常处置服务 9
9.3　越权、伪造令牌、黑名单拦截处置服务 10
10　交易存证、对账与档案管理服务 10
10.1　全链路存证服务要求 10
10.2　交易对账服务要求 10
10.3　电子档案归档与保管服务 10
11　平台运营服务要求 10
11.1　智能体平台运营服务 10

11.2 商户入驻与商品目录管理服务.....11
11.3 用户咨询、投诉与纠纷处理服务.....11
11.4 日常巡检与系统运维服务.....11
12 安全合规服务要求.....11
12.1 用户隐私保护服务.....11
12.2 反洗钱与交易合规服务.....11
12.3 国密加密与身份认证服务.....11
12.4 应急处置服务.....11
13 服务评价与持续改进.....12
13.1 评价维度.....12
13.2 评价实施流程.....12
13.3 问题整改与服务优化.....12
参考文献.....13

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。

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。

本文件由苏州金服产业运营服务有限公司提出。

本文件由苏州市金融业商会归口。

本文件起草单位：苏州金服产业运营服务有限公司、江苏金服数字集团人工智能科技有限公司、江苏金服数字集团苏州金服产业运营服务有限公司、中国建设银行苏州分行、麦斯达夫（苏州）科技集团有限公司。

本文件主要起草人：何国星、李萍、卞国春、刘云、高文义、杨凡、姚海峰、李宝镖、杜开洪、张怡轩、孙波波、金明、戴天丽、张正方、韦三纲、谢婷婷、李宁。

数字人民币智能体交易服务规范

1 范围

本文件规定了数字人民币多智能体交易服务的基本要求、智能体全生命周期管理、前置授权服务、交易场景服务、风险管控专项服务、交易存证、对账与档案管理服务、平台运营服务要求、安全合规服务要求和服务评价与持续改进等服务要求。

本文件适用于为个人用户、企事业单位、个体工商户提供服务的主体建设与运营的数字人民币多智能体自动化交易系统。

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/Z 185.1—2026 人工智能 智能体互联 第1部分：总体架构

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 43580—2023 区块链和分布式记账技术 存证通用服务指南

GB/T 42929—2023 互联网金融智能风险防控技术要求

GM/T 0054—2018 信息系统密码应用基本要求

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0197—2020 金融数据安全 数据安全分级指南

ISO 20022 A single standar disation approach (methodology, process, repository) to be used by all financial standards initiatives

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字人民币智能体交易 e-CNY agent-based tansaction

由智能体执行的数字人民币自动化交易业务。

3.2

AI 智付 AI-pay platform

面向数字人民币智能体交易（3.1）的城市级数字人民币综合服务平台。

3.3

支付委托书 payment mandate

用户向数字人民币智能体交易（3.1）服务提交的、用于自动化智付业务授权的有效业务文件。

3.4

支付令牌 payment token

基于有效支付委托书（3.3）生成的单次交易短期业务执行凭证。

4 缩略语

下列缩略语适用于本文件。

e-CNY：数字人民币（electronic chinese yuan）

MCP：多智能体通信协议（multi-agent communication protocol）

ACT：多智能体协作协议（multi-agent collaboration protoco）

5 基本要求

5.1 服务原则

5.1.1 合规性

平台、全部注册智能体、入驻商户、终端用户应遵循数字人民币、支付监管、人工智能、数据安全相关法律法规；智能体注册、支付交易、资金清算、风控数据报送全流程应落实监管备案相关服务。个人信息、金融数据保护相关服务应符合GB/T 35273—2020、JR/T 0171—2020、JR/T 0197—2020相关服务要求；多智能体互联协同服务宜参考GB/Z 185.1—2026给出的总体架构思路开展建设；风险防控相关服务应符合GB/T 42929—2023相关服务要求。

5.1.2 安全可控

应采用“委托书+短期令牌”二级最小授权隔离服务模式，服务过程应对智能体越权操作予以拦截；宜同步搭建智能体身份、网络传输、交易支付、资金存储、数据存储五层安全服务防护，落实交易防篡改、全链路可追溯、全节点可审计的服务要求。

5.1.3 智能性

应依托大模型完成自然语言需求自动拆解、子任务拆分、智能体匹配调度；宜支持跨智能体协同联动，通过一次性长期授权替代重复人工操作，提升交易自动化、业务处理效率。。

5.1.4 便捷性

全部交易关键节点应开展区块链存证服务；智能体审核标准、风控阈值、清算周期、平台收费规则应全面对外公示；宜提供H5、客户端、服务通道多端接入服务，简化智能体注册、商户入驻、用户授权操作门槛。

5.1.5 公平性

用户钱包私钥、核心敏感信息应留存于本地客户端，平台仅临时持有短期支付令牌；应统一智能体准入、商户结算、用户风控服务标准，宜避免出现差异化歧视服务。

5.1.6 开放性

应兼容ACT协作协议、MCP统一通信协议，标准化智能体注册、支付对接服务；宜开放开发文档与工具，鼓励第三方开发者、金融机构、实体商户共建智能体互联网产业生态。

5.2 参与主体及权责

5.2.1 用户

用户包含委托人、个人和对公企业人员，其权责包含以下内容：

a) 完成实名钱包开立，对公额外完成营业执照、法人资质核验；
b) 自主配置支付委托书全部额度、用途、时效、收付款约束，自主设置 L3 大额审批阈值；
c) L3 大额、L2 高风险交易及时完成钱包确认/驳回，超时效未处理自动取消订单；
d) 随时查询委托书、全量交易流水、区块链存证凭证，针对资金、履约争议发起咨询投诉；
e) 妥善保管钱包登录、国密签名密钥，自身泄露、不当授权引发资金风险自行承担；
f) 企事业单位用户，可在支付委托书中配置 L3 大额交易多角色协同审批规则，定义审批角色、审批类型、审批流转顺序、整体审批时效约束。

5.2.2 AI 智付平台运营服务商

AI智付平台运营服务商权责包含以下内容：

a) 搭建分布式高可用智能体互联网底座，配置满足本标准能力指标的多智能体编排引擎，部署五个核心功能模块、四类基础业务智能体；
b) 建立商户智能体、通用服务智能体、数币智能体完整生命周期管理，统一 MCP 三类接入模式标准；
c) 应严格执行授权、四类交易、清算退款、分级风控全流程服务，宜避免跳过强制校验、存证相关服务节点；

d) 落地网络、数据、智能体、资金四层安全保障服务，智能交互、支付行为应完整留存业务日志；
e) 配套商户一站式入驻、培训、技术支持、营销推广、纠纷调解全流程服务；
f) 提供 7×24h 智能体调用、资金流向监控服务，分级开展风险处置，按期向监管报送智能体接入、交易流水、风控处置等全套业务资料；
g) 运营开发者社区，开展产业场景协同、标准共建服务；
h) 按月开展内部自查服务，每半年组织第三方联合评价服务，配合监管、审计调取完整存证资料，宜避免隐匿篡改业务记录。

5.2.3 注册智能体主体

注册智能体主体包含商户智能体、服务智能体和数币智能体，其权责内容包含以下内容；
a) 商户智能体：
   1) 完成工商、数字人民币收款资质备案及 MCP 平台注册服务；
   2) 结构化上架商品目录，真实上报履约签收相关业务事件；
   3) 接收自动数字人民币结算服务，配合 T+1 对账、智能合约整单或部分退款服务；
   4) 定期参与平台安全、能力评级服务，出现不合格情形宜限期开展整改服务。
b) 通用服务智能体：
   1) 提交完整注册资质，遵循 MCP 交互服务规范，保障服务响应时效；
   2) 开放标准化付费服务通道，配合智能体间小额自动结算服务；
   3) 交互业务日志留存期限应不少于 3 年。
c) 数币智能体：数币智能体：由平台专属资质主体开展运营服务，独立承担商户资质核验、支付指令下发、资金清算、智能合约触发、退款核销、交易风险识别相关服务。

5.2.4 数字人民币运营机构

数字人民币运营机构权责内容包含以下内容：
a) 开放标准化数字人民币支付、智能合约服务，业务报文宜遵循 ISO 20022 相关要求；
b) 负责底层资金划转、交易状态同步服务，支持 T+0 实时清算、商户约定周期结算服务；
c) 开展全量资金动态监测服务，识别大额、可疑交易，按期向监管报送反洗钱相关业务资料。

5.2.5 区块链存证机构

区块链存证机构权责内容包含以下内容：
a) 对接存证智能体标准化上链接口，接收委托书、交易、审批、风险处置全链路事件，提供分布式不可篡改存储服务；
b) 提供哈希完整性校验、电子审计凭证导出、线上验真服务；
c) 按金融档案要求长期存储存证数据，支持多维度检索调取，禁止删除覆盖原始记录。

5.3 服务分层框架

系统整体采用四层递进式服务架构，各层级服务边界清晰、自上而下单向驱动业务流转，层级间通过标准化接口完成交互，整体形成闭环服务体系；
a) 用户入口服务层：面向终端用户、商户、运营管理人员提供可视化操作服务，承担用户发起授权、发布交易需求、审批确认、查询对账、投诉反馈等前端交互服务；
b) 多智能体协作服务层：核心业务调度服务层，由授权智能体、交易智能体、支付智能体、存证智能体四类组件协同提供专业化服务，系统应配置多智能体编排引擎，应满足以下服务能力指标：
   1) 作为四类智能体之间业务交互的唯一业务数据中枢，统一归集委托书信息、交易需求信息、交易提案信息、支付令牌信息、审批处置信息、交易状态信息等核心业务主数据；
   2) 开展数据一致性保障服务，当多智能体并行开展 9 项授权边界强制校验、多任务并发调度场景下，中心化主数据服务对业务状态进行统一管控，保障不同智能体读取、引用的业务主数据版本统一，宜规避多智能体并行处理引发的业务状态冲突、数据不一致问题；

3) 开展状态同步服务，四类智能体产生的业务状态变更，应首先更新至中心化主数据服务，再向其他关联智能体分发业务状态变更通知，宜避免智能体之间直接跨组件私自传递核心业务主数据；
4) 开展读写隔离服务，区分主数据查询服务与主数据变更服务，高并发查询场景提供多路径查询服务，业务状态变更执行统一管控，保障业务状态变更的有序性；
5) 开展可追溯服务，主数据服务内全部业务数据变更过程留存完整业务操作轨迹，轨迹信息同步推送至存证服务，支持后续审计核查服务。

c) MCP 工具支撑服务层：标准化工具底座服务，统一提供以下六项金融服务能力，为上层智能体提供标准化服务调用支撑，统一服务调用规范与服务异常处理规则：
1) 数字人民币支付服务；
2) 数字人民币智能合约服务；
3) 区块链存证服务；
4) 身份核验服务；
5) 商品目录查询服务；
6) 物联网资产可信数据服务。

d) 外部系统对接服务层：对外互通服务层，提供标准化对接通道，实现与官方数字人民币支付系统、数币智能合约平台、第三方区块链存证平台、公安/市场监管身份认证系统安全对接，完成跨系统数据、指令交互服务。

5.4 分级管控规则

平台应基于用户支付委托书额度、交易场景、风险标签建立三级分级管控机制，分为L1、L2、L3管控阈值支持用户自主配置，系统自动识别交易等级并执行对应服务流程：

a) L1 常规小额交易：交易金额低于委托书单笔风险阈值、用途为白名单常规采购、无风险标签，系统自动完成 9 项授权边界校验，校验通过后直接放行支付，无需人工干预，全程自动化执行；

b) L2 预警交易：交易金额接近单笔、单日、总额授权上限、用途包含风险关键词、收款方为新增陌生商户、短期高频发起同类交易，系统宜不阻断支付，实时向用户钱包推送风险提醒通知，告知交易潜在风险，留存预警记录并开展存证服务；

c) L3 大额审批交易：单笔交易金额超过用户设定的委托书单笔阈值，支付流程自动临时挂起，暂停资金划转操作；由用户在数字人民币钱包完成手动确认后方可继续支付，用户选择驳回则终止订单，全部审批操作宜开展全程存证归档服务。

5.5 委托代理与风险责任服务规则

开展数字人民币智能体交易服务，应当依托用户出具的支付委托书建立委托代理业务关系，对齐民事委托代理相关法律要求，落实以下服务规则；

a) 支付委托书业务性质与授权范围限定：
1) 支付委托书是用户作出委托代理授权意思表示的业务载体，是智能体开展自动化支付的业务授权凭证；
2) 平台服务应当强制要求支付委托书明确载明代理事项、单笔/周期支付额度上限、允许及禁止的交易用途、可收款主体范围、有效期、审批流转规则；不得支持无明确边界的概括式全权授权；
3) 委托书发生变更、续期、吊销时，代理授权同步发生变更或终止；系统应当同步作废全部未到期支付令牌，阻断已终止授权下的全部智能体交易。

b) 智能体支付指令的委托代理业务拟制：
1) 在支付委托书载明的授权边界内，由智能体按照业务规则自动生成并下发的数字人民币支付指令，业务上视为用户委托代理之下的意思表示延伸；
2) 全部自动支付行为必须以有效、未吊销、未过期的支付委托书及对应单次支付令牌为前提；超出委托书载明约束的，不产生该等委托代理业务效力；

3) 委托书开立、变更、吊销、每一笔自动支付的关键业务节点均完成存证归档，作为判断代理授权状态的业务凭证。

c) 越权交易、误操作造成资金损失的风险处置与责任分担服务要求：

1) 发生资金损失争议时，平台应向用户、监管、纠纷调解主体完整提供区块链存证业务凭证，支撑责任判定与纠纷处理服务；

2) 平台应在用户服务协议、委托书展示页面，以显著方式向用户提示智能体自动化交易模式下的代理关系、风险边界与各方责任提示服务。

5.6 跨域数据流转与数据不出域服务规则

平台应当落实数据不出域安全原则，清晰划分业务域边界，区分原始敏感业务数据与摘要、哈希校验类非敏感凭证信息，在满足存证、监管报送、对账等法定及业务必需跨机构交互场景下执行以下服务规则；

a) 业务域划分定义：

1) 用户客户端域：用户数字人民币钱包客户端本地运行环境，用户钱包私钥等核心敏感信息留存于此域；

2) 智能体执行域：各注册智能体独立运行的业务服务环境，各智能体之间执行必要的数据隔离；

3) 平台运营域：AI 智付平台运营服务商统一管控的业务运行、数据存储、业务处理服务环境。

b) 数据不出域原则边界：

1) 原始敏感业务数据不出域：包含用户身份标识、完整交易明细、钱包敏感凭证等原始敏感业务数据，原则上不离开所属业务域；

2) 脱敏摘要、哈希校验值可跨域流转：用于存证验真、交易核验的哈希摘要、汇总统计类脱敏加工后数据，不属于原始敏感业务数据，可按业务需要跨机构流转；

3) 法律法规、监管制度明确要求报送数据的情形，按照监管规定执行。

c) 跨机构数据流转服务约束：

1) 最小必要：跨机构对外提供数据，仅输出业务履行、监管履职所必需的最小范围数据，不得超业务目的传输原始敏感业务数据；

2) 传输安全：跨机构数据交互应当采用加密传输服务，保障传输过程数据保密性、完整性；

3) 接收方安全义务：与外部存证机构、监管报送接收机构、对账合作机构开展业务协作时，应当通过服务协议明确接收方的数据安全保管、使用范围、留存期限、事件告知等义务；

4) 流转留痕：全部跨机构数据输出行为留存完整业务轨迹，支持审计核查。

d) 典型业务场景适配说明：

1) 区块链存证业务：向外输出存证哈希、业务事件摘要，原始敏感业务数据保留在平台运营域；

2) 监管反洗钱报送业务：按监管要求输出脱敏汇总报表、可疑交易线索，严格遵循监管报送口径；

3) 资金对账业务：与数字人民币运营机构开展对账交互，按照对账业务最小必要原则交互对账要素。

6 智能体全生命周期管理

6.1 智能体注册

6.1.1 注册主体分类

注册主体分类如下：

a) 商户智能体：合规经营企业、个体工商户或其合作开发机构；

b) 通用服务智能体：具备软件开发、服务运营资质的科技企业、科研机构、第三方开发者；

c) 数币智能体：仅由平台指定具备支付合规资质的主体注册运营。

6.1.2 注册必备资料

应根据要求提供注册必备资料，内容包含以下内容：

a) 基础信息：智能体唯一名称、类型、运营主体、联系方式、统一社会信用代码；
b) 能力信息：覆盖业务场景、功能清单、支持 MCP 协议类型、接口规范、响应性能指标；
c) 资质文件：主体营业执照、行业经营许可；
d) 合规承诺文件：签署数据安全、合规经营、服务质量承诺书。

6.1.3 注册 6 步流程

注册分为6步，具体流程如下：

a) 提交申请：平台线上填报资料，自主选择 stdio、streamable、开放服务通道任一 MCP 注册服务模式；
b) 资料初审：平台校验材料完整性、格式规范、信息一致性，资料缺失时宜一次性告知开展补全服务；
c) 联合资质审核：联合金融、监管机构核验主体合规性、无失信涉诉记录，必要时宜开展实地核查、安全能力评估服务；
d) 平台备案：审核通过分配全局唯一智能体标识、开通对应接口访问权限，同步录入监管备案台账；
e) 功能安全测试：开展服务连通、业务功能、安全能力全量评估服务；
f) 正式上线：评估合格纳入智能体互联网服务体系，开放对外交互调用服务。

6.2 智能体评级认证与动态处置

6.2.1 安全四级维度评级

从身份认证安全、传输数据安全、跨智能体交互安全、支付结算安全四大维度综合打分，划分一级、二级和三级，分别为基础安全、中间安全和高级安全。

6.2.2 能力五级维度评测

从功能准确性、接口响应性能、多智能体协同能力、长期服务稳定性、用户使用体验划分优、合格、不合格三级能力。

6.2.3 认证复核与分级处置

平台定期（每季度）开展评级复核，根据等级执行差异化管控：

a) 轻微不合格：开展书面告知、限期整改、限制调用频次服务；
b) 一般不合格：临时暂停智能体对外服务，整改复核通过后方可恢复服务；
c) 严重不合格：注销智能体接入服务权限，同步更新监管备案信息。

7 前置授权服务

7.1 用户身份核验服务

用户身份核验服务为智能体互联网交易准入第一道流程，仅完成实名与经营资质双重核验的用户，方可开通全部智能支付权限，核验环节采用权威官方系统对接，内容如下：

a) 用户打开数字人民币钱包，进入智能体交易服务开通模块，提交开通申请，同步上传实名、资质材料；
b) 平台自动调用身份核验 MCP 工具，对接权威身份认证系统完成自然人实名核验、企业工商资质核验，校验经营范围、经营状态是否合规；
c) 核验全部材料真实有效、无异常风险记录后，为用户开通智能体交易全部服务权限；核验不通过时，系统一次性完整告知缺失材料、不合规项。

7.2 支付委托书开立服务

规范委托书参数配置、文本确认、数字签名、上链存证、回执发放全套标准操作，所有授权约束由用户自主设置、自主确认，具体流程如下：

a) 用户在钱包可视化界面逐项录入完整授权参数，包括单笔支付上限、单日累计支付上限、委托书有效期内总额上限、支付用途白名单、禁止支付用途黑名单、允许收款方主体类型、禁止收款方名单、合约支付权限开关；所有参数配置项附带说明文字，提示额度管控风险；
b) 系统完整展示标准化支付委托书全文，清晰列明全部授权约束、资金风险、存证规则，用户阅读确认后使用钱包国密算法完成数字签名，签名文件作为授权生效法定凭证，密码应用保障应符合 GM/T 0054—2018 的相关服务要求；
c) 授权智能体生成全局唯一委托书编号，同步将委托书原始文件、用户签名记录推送至存证智能体执行区块链上链存证；
d) 委托书生效后，系统向用户生成电子回执单，回执包含完整授权参数、存证哈希值，支持用户在钱包内随时查看、下载、导出、打印归档服务。

7.3 委托书变更、续期、吊销服务

委托书生效后支持动态调整有效期、额度、收付款约束，同时设置到期自动失效、风险强制吊销机制，统一变更、续期、吊销三类操作业务流程如下：

a) 变更服务：用户需要调整额度、用途、有效期、黑白名单时，可发起委托书变更申请；修改完成后需重新进行国密数字签名，原委托书标记为失效归档，系统生成全新有效委托书，新旧委托书关联存证；
b) 续期服务：委托书有效期届满前 30 天内，用户可发起续期申请，无需重复录入全部授权参数，仅调整新有效期并签名确认即可；过期未续期委托书自动失效；
c) 吊销服务：用户主动申请注销授权、委托书有效期自然到期、系统识别用户存在高风险违规交易时，授权智能体立即吊销对应委托书，同步批量作废该委托书下所有未过期支付令牌，阻断后续所有智能体支付服务；
d) 委托书开立、变更、吊销、续期全流程操作记录、用户签名、系统处置日志统一开展区块链存证服务，存证保管期限应不少于 5 年，支持长期审计调取服务。

7.4 支付令牌签发与生命周期管理服务

支付令牌是单次交易短期执行凭证，依托委托书生成、有效期严格管控，实现“长期委托书+单次短期令牌”二级隔离安全机制，令牌生成、绑定、失效、校验全流程如下：

a) 用户发起单次智能体交易需求，全局调度授权智能体先校验对应委托书状态为有效、未吊销、未过期，校验通过后方可生成单次交易专用短期支付令牌；
b) 支付令牌强制绑定本次交易唯一信息：交易金额、支付用途、收款方主体、委托用户、委托书编号，令牌固定有效期 5 分钟，到期自动失效；
c) 出现令牌过期、对应委托书吊销、用户主动取消交易、支付流程终止任一情形，令牌即时标记作废，永久不可复用；
d) 支付智能体发起数币划转前首先校验令牌有效性，失效、伪造、过期令牌直接拦截支付流程，同步向用户推送拦截原因通知并留存风险记录。

7.5 授权边界校验服务

支付智能体执行数字人民币资金划转操作前，系统引擎按顺序完成9项强制校验，采用串行校验逻辑，任意一项校验不通过则终止交易，同步推送失败原因至用户钱包，所有校验记录上链存证：

a) 校验支付令牌国密数字签名合法有效，宜规避篡改、伪造痕迹；
b) 校验当前系统时间未超出令牌有效期限；
c) 校验本次交易单笔金额不高于委托书设定单笔支付上限；
d) 校验用户当日已支付累计金额加上本次交易金额不高于委托书单日累计上限；
e) 校验委托书周期内历史总支付金额加上本次交易金额不高于委托书总额上限；
f) 校验本次交易用途落在委托书约定用途白名单范围内；
g) 校验本次交易用途未出现在委托书禁止支付黑名单；
h) 校验收款方主体类型符合委托书允许收款方类型要求；

i） 校验本次收款方未列入委托书禁止收款方黑名单。

8 交易场景服务

8.1 S1 用户委托自动支付服务

S1用户委托自动支付服务流程如下：

a） 用户在数字人民币钱包输入自然语言采购/支付需求，需求指令推送至交易智能体；
b） 全局编排引擎自动拆解完整业务任务，并行启动两条业务链路：交易智能体调用商品目录 MCP 工具完成供应商匹配、商品比价、交易条件协商；授权智能体并行预校验委托书基础有效性，提前拦截明显越权交易服务；
c） 交易智能体完成商品、价格、收款方协商确认，生成完整交易方案，授权智能体依据交易方案生成本次交易专用短期支付令牌；
d） 支付智能体携带合法有效支付令牌，调用数币支付 MCP 工具向数字人民币系统下发资金划转指令；
e） 数字人民币系统返回成功或失败状态，支付结果同步推送交易智能体与存证智能体，存证智能体将完整交易事件开展区块链锚定存证服务；
f） 用户数字人民币钱包接收交易完成推送通知，通知清晰展示交易金额、收款方名称、支付用途、交易流水号、存证查询入；
g） 授权 9 项校验任意失败、数币系统返回支付失败时，系统自动终止全部订单流程，向用户推送标准化失败原因，完整异常日志留存存证服务。

8.2 S2 用户确认式智能支付服务

S2用户确认式智能支付服务流程如下：

a） 交易智能体接收用户支付需求，完成商品匹配、价格协商，生成标准化交易提案，提案包含商品明细、总金额、收款方、支付用途、预计消耗授权额度；
b） 系统将完整交易提案推送至用户数字人民币钱包，弹窗提示人工复核，等待用户操作；
c） 用户点击确认交易：系统进入支付令牌签发、资金自动划转标准流程；
d） 用户点击驳回交易：交易立即终止，系统记录驳回时间、用户操作记录，同步上链存证；
e） 超时处置规则：提案推送后 30 min 内用户未执行确认/驳回操作，系统自动取消本次交易，释放占用授权额度，留存超时记录。

8.3 S3 智能体间 API 小额付费服务

S3智能体间API小额付费服务流程如下：

a） 发起方智能体 A 调用服务提供方智能体 B 付费服务通道，同步携带交易需求、委托用户标识、支付用途；
b） 授权智能体调取用户有效委托书，校验委托书已开通智能体间小额付费权限、交易未超出授权约束；
c） 校验通过后生成小额短期支付令牌，支付智能体自动执行数字人民币小额资金划转；
d） 资金支付成功后，智能体 B 正常返回服务结果；支付失败则立即终止服务调用，平台触发运行告警，同步告知委托用户；
e） 所有智能体间小额交易统一归集，每日 T+1 自动生成跨智能体结算汇总清单，支持平台、商户对账导出。

8.4 S4 数字人民币智能合约条件支付服务

8.4.1 用户通过钱包向授权智能体发起合约支付配置申请，设置结构化履约触发条件。履约触发支持两类服务模式：

a） 模式一：业务主体履约事件上报服务；
b） 模式二：物联网资产数据服务。面向新能源重卡以租代购等重资产运营场景，提供资产运行数据与智能合约、数字人民币服务通证化结算的自动化绑定服务。物联网资产数据服务应当遵循

统一服务接入规范，完成资产身份核验、数据可信校验，仅经核验通过的资产数据可作为合约触发依据。

8.4.2 交易智能体生成标准化电子采购/租赁类电子合同，合同应完整载明以下内容：

a) 商品或重资产相关信息；
b) 交易金额；
c) 履约规则；
d) 资产数据服务相关约束。

8.4.3 支付智能体将用户设置的结构化触发条件、资产服务绑定关系、数据校验服务要求写入数字人民币智能合约服务平台。

8.4.4 合约创建完成后服务状态标记为“待条件触发”，以下关键业务环节同步开展区块链存证服务：

a) 合约创建；
b) 合约参数配置；
c) 资产服务绑定关系确认；
d) 用户签名确认。

8.4.5 合约履约触发分为两条服务路径，满足对应路径全部履约条件即可触发资金划转：

a) 路径一：商户/履约方开展货物签收、验收完成等履约事件上报服务；
b) 路径二：物联网资产数据服务提供方上报重资产运行、使用、状态等可信资产数据服务。

8.4.6 数字人民币智能合约服务平台校验履约条件全部达成后，主动触发支付智能体执行资金划转服务，支持服务通证化结算场景下的分期结算、按资产实际使用量自动结算。

8.4.7 合约约定有效期内，未收到合规履约事件、履约条件未能达成的：

a) 合约自动到期冻结；
b) 向用户推送业务通知；
c) 为用户提供两项处置选择：申请合约续期服务、直接撤销合约服务。

9 风险管控专项服务

9.1 L3 大额人工审批服务

L3大额人工审批服务流程如下；

a) 支付智能体解析本次交易金额，对比委托书单笔风险阈值，识别金额超限时自动挂起支付指令，暂停资金划转；
b) 全局编排引擎自动生成标准化审批单据，单据包含委托书编号、交易明细、占用额度、风险等级提示、审批时效说明；
c) 审批单据实时推送至用户数字人民币钱包，提供专门审批操作入口，审批模式区分个人用户模式与企事业单位多角色协同审批模式：
   1) 个人用户模式：审批单据推送至用户数字人民币钱包，由该用户独立完成审批操作；
   2) 企事业单位多角色协同审批模式：支持串行审批、会签审批两种审批流程，可按单位内部权责分工配置审批角色。
d) 各审批角色仅可执行二选一操作：确认支付、驳回交易；企事业单位场景下，任意审批角色选择驳回，整笔交易直接作废；
e) 个人用户确认支付/企事业单位全部规定审批节点完成确认：流程恢复，签发支付令牌执行划转；
f) 任意审批主体驳回：订单直接作废，释放授权额度；
g) 审批通知推送、用户操作记录、审批最终结果、处置时间全部作为独立节点上链存证，永久留存审计凭证。

9.2 交易异常处置服务

交易异常处置方法如下：

a) 支付失败处置：数字人民币系统返回资金划转失败时，系统自动发起资金回滚校验，确认资金原路退回用户钱包，同步向用户、商户推送失败通知；

b) 系统超时处置：数币接口、智能合约平台通信超时，自动执行 3 次间隔重试，重试全部失败后终止交易，完整留存超时日志、接口返回报文作为异常凭证；
c) 对账不平处置：T+1 系统自动执行用户、商户、平台三方流水自动对账，识别资金差异数据自动标记，推送运营人员人工核对、完成调账，差异处置记录归档。

9.3 越权、伪造令牌、黑名单拦截处置服务

越权、伪造令牌、黑名单拦截处置服务操作方法如下：
a) 越权交易拦截：授权校验引擎识别交易超出额度、用途、收款方约束，立即拦截全流程交易，锁定本次交易记录，向用户推送高风险提醒；
b) 伪造令牌拦截：校验发现令牌 SM2 签名不合法、令牌参数被篡改，系统触发平台一级安全告警，临时冻结用户智能体支付权限，留存伪造令牌原始数据用于风险核查；
c) 黑名单拦截：收款方主体命中用户黑名单、行业风险商户黑名单，直接终止交易，同步录入平台风险台账，定期汇总黑名单交易上报监管。

10 交易存证、对账与档案管理服务

10.1 全链路存证服务要求

10.1.1 平台强制设置 6 个不可省略的区块链存证节点，每一个节点业务事件生成标准结构化存证报文，实时推送区块链存证机构完成哈希锚定，数据不可篡改、不可删除：
a) 支付委托书签发及用户数字签名事件；
b) 用户交易需求发起、交易提案生成事件；
c) 授权智能体执行 9 项授权边界校验事件；
d) 单次交易支付令牌签发、作废事件；
e) 数字人民币支付成功/失败执行结果事件；
f) L3 大额交易人工审批操作事件。

10.1.2 存证原始数据、区块链哈希凭证保管期限不少于 5 年，支持用户、监管机构凭有效身份凭证按需线上调取、核验存证文件。

10.1.3 区块链存证业务开展，存证业务流程、凭证管理宜符合 GB/T 43580—2023 的相关服务要求。

10.2 交易对账服务要求

交易对账服务要求如下：
a) 每日 T+1 系统自动批量生成三类标准化流水文件：用户个人或企业全量交易流水、商户结算收款流水、智能体间付费服务通道结算流水；
b) 系统内置自动对账引擎，完成平台交易记录与数字人民币底层资金流水交叉比对，对账差异数据自动高亮标记，推送运营人员人工核查处置；
c) 所有对账文件支持电子表格、PDF 标准化导出服务，文件附带平台电子签章，具备对账凭证效力。

10.3 电子档案归档与保管服务

电子档案归档与保管要求如下：
a) 将支付委托书、电子交易合同、区块链存证哈希凭证、L3 审批记录、异常处置日志、对账单据统一归集为电子档案，分类归档；
b) 电子档案采用国密加密存储，设置分级访问权限，普通用户仅可查看本人档案，运营、审计人员凭权限调取全量档案；
c) 支持档案按时间、委托书编号、交易金额、商户名称多维度检索，批量导出档案用于交易纠纷举证、监管审计。

11 平台运营服务要求

11.1 智能体平台运营服务

11.1.1　应保障授权智能体、交易智能体、支付智能体、存证智能体四类组件 7×24 h 不间断稳定运行，设置多实例容灾备份。
11.1.2　全局编排引擎内置故障自动降级、流量熔断保护机制，接口并发峰值、组件异常时自动限制交易量，避免全平台瘫痪。
11.1.3　应按月更新授权校验规则库、商户风险黑名单、高风险用途关键词库，同步公示规则更新内容。

11.2　商户入驻与商品目录管理服务

11.2.1　商户入驻应实行一站式线上资质核验服务，一次性提交材料完成工商、经营资质校验，缩短入驻周期。
11.2.2　应统一商品目录结构化数据标准，强制规范品类、单价、履约周期字段，适配交易智能体自动比价、需求匹配。
11.2.3　应为商户提供结算周期自定义、每日自动对账、电子发票推送配套运营服务。

11.3　用户咨询、投诉与纠纷处理服务

11.3.1　搭建 App 在线客服、服务热线双通道咨询渠道，常规额度查询、流程咨询诉求 15 min 内响应回复。
11.3.2　交易资金、授权、存证类纠纷正式受理后，3 个工作日内调取完整区块链存证凭证完成事实核查，并向用户反馈核查结果。
11.3.3　应建立全量投诉电子化台账，按月汇总投诉类型、问题成因，复盘优化平台交易服务流程。

11.4　日常巡检与系统运维服务

11.4.1　运维人员应每日定时巡检四类智能体运行状态、授权校验引擎可用性、数字人民币接口连通性，形成每日巡检日志。
11.4.2　每月开展一次安全专项巡检，每季度开展四大交易场景全链路压力测试，提前识别并发、稳定性隐患。
11.4.3　系统版本迭代、规则更新提前 3 个工作日公示告知用户，预留业务缓冲期，避开企业集中采购结算高峰。

12　安全合规服务要求

12.1　用户隐私保护服务

应遵循个人信息最小采集原则，仅收集开展智能体交易必需的身份、资金参数，不采集无关隐私信息；身份证号、银行卡、交易金额等敏感字段在传输、存储环节全程脱敏，并采用SM4对称加密保护。未经用户书面授权，不得向商户、第三方机构、合作服务商共享、泄露用户交易、授权隐私数据。

12.2　反洗钱与交易合规服务

12.2.1　系统应内置交易监测模型，对大额、连续高频、跨陌生商户、夜间异常交易自动预警，运营人员复核留存预警台账。
12.2.2　应按照人民银行反洗钱监管周期要求，定期汇总交易统计报表、可疑风险台账报送监管机构。
12.2.3　系统强制拦截投资理财、虚拟货币交易、非法金融活动等黑名单用途的智能体支付请求。

12.3　国密加密与身份认证服务

12.3.1　平台与钱包、商户、数币系统之间全部交易报文应采用 SM2 国密非对称签名、SM4 国密对称加密传输，配套双向 TLS 通信认证；
12.3.2　四类智能体应基于 PKI 公钥基础设施数字证书完成身份认证，杜绝伪造智能体接入系统。
12.3.3　用户开立、变更委托书、确认 L3 大额审批等高风险操作，使用数字人民币钱包完成 SM2 数字签名，无签名操作不予生效。

12.4　应急处置服务

12.4.1　平台应编制完整应急预案，覆盖系统宕机、数币接口中断、批量越权异常交易、数据泄露等突

发事件。

12.4.2 发生安全、资金风险事件时，系统自动暂停全部智能体支付服务，第一时间推送通知告知用户，并同步上报属地金融监管机构。

12.4.3 应急处置完成后 5 个工作日内形成完整复盘报告，记录事件起因、处置流程、损失情况、优化整改措施，统一归档留存。

13 服务评价与持续改进

13.1 评价维度

开展智能体交易服务质量评价时，应覆盖四大核心维度，逐项对照本标准条款核查：

a) 流程规范性：授权开立、四大交易场景、风控审批、存证归档全流程是否完整遵循本标准规定步骤，无缺项、简化操作；

b) 服务时效：客服咨询响应速度、支付指令处理时长、交易纠纷核查处理周期、版本更新通知时效；

c) 安全合规：二级授权校验、国密加密、区块链存证、反洗钱风控、隐私保护等合规措施落地执行情况；

d) 用户满意度：操作便捷度、消息通知清晰度、异常问题处置体验、对账与凭证获取便利性。

13.2 评价实施流程

智能体平台运营服务商按月开展内部合规自评，对照标准形成月度自评报告；每半年组织用户代表、入驻商户、第三方标准化机构开展联合外部服务质量评价；金融监管、行业标准化机构可依据本标准全部条款，对平台开展合规专项评价核查。

13.3 问题整改与服务优化

13.3.1 自评、外部评价、监管核查发现不符合标准的事项，应建立专项整改台账，明确整改措施、完成时限、责任人，限期闭环验收。

13.3.2 常态化收集企业用户、商户操作优化建议，迭代优化智能体交互流程、钱包操作界面、风控提醒机制。

参 考 文 献

[1] 中华人民共和国第十二届全国人民代表大会常务委员会。中华人民共和国网络安全法[Z].2016-11-07（2017-06-01施行）.

[2] 中华人民共和国第十三届全国人民代表大会常务委员会。中华人民共和国数据安全法[Z].2021-06-10（2021-09-01施行）.

[3] 中华人民共和国第十三届全国人民代表大会常务委员会。中华人民共和国个人信息保护法[Z]. 2021-08-20（2021-11-01 施行）.

[4] 中华人民共和国第十四届全国人民代表大会常务委员会。中华人民共和国反洗钱法[Z].2024-11-08（2025-01-01施行）.

[5] 中华人民共和国第十二届全国人民代表大会常务委员会。中华人民共和国消费者权益保护法[Z].2013-10-25（2014-03-15施行）.

[6] 中华人民共和国第十届全国人民代表大会常务委员会。中华人民共和国中国人民银行法[Z].2003-12-27修正（2004-02-01施行）.

[7] 中华人民共和国国务院。非银行支付机构监督管理条例[Z].国务院令第768号，2023-12-09（2024-05-01施行）.

[8] 中国人民银行。金融机构大额交易和可疑交易报告管理办法[Z].中国人民银行令〔2016〕第3号，2016-12-28（2017-07-01施行）.

[9] 中国人民银行，中国银行业监督管理委员会，中国证券监督管理委员会，中国保险监督管理委员会。金融机构客户身份识别和客户身份资料及交易记录保存管理办法[Z].〔2007〕第2号令，2007-06-21（2007-08-01施行）.

[10] 中国人民银行。中国人民银行金融消费者权益保护实施办法[Z].中国人民银行令〔2020〕第5号，2020-09-15（2020-11-01施行）.

[11] 中国人民银行。关于进一步加强数字人民币管理服务体系和相关金融基础设施建设的行动方案[Z].2025-12-29（2026-01-01实施）.