《数字人民币智能体交易服务规范》
团体标准编制说明

一、立项的意义

（一）立项背景

当前数字人民币试点应用持续深化，人工智能多智能体技术逐步落地各类金融、民生交易场景，依托智能体自主完成商品筛选、交易协商、自动支付、履约分账的新型自动化交易模式快速兴起。个人、企事业单位、个体工商户可通过授权智能体替代人工完成重复性、周期性交易操作，大幅降低交易运营成本，但行业尚未形成统一技术约束与安全管控体系，存在多重现实痛点。

一是智能体交易底层架构无统一规范，各机构自研系统架构差异巨大，用户授权机制、智能体调度逻辑、支付交互接口不兼容，跨平台、跨机构智能体协同交易难以落地，存量金融多智能体平台复用缺少标准化集成路径，重复开发、资源浪费问题突出。二是资金授权安全体系缺失，市场普遍存在单层授权模式，缺少长期委托书+短期支付令牌双层防护机制，交易额度、收款方、资金用途管控颗粒度粗放，超授权交易、伪造支付指令、资金挪用风险难以防控。三是交易全流程可追溯能力不足，多数智能体交易系统仅留存简易操作日志，未覆盖授权签发、交易协商、支付执行、合约触发全节点区块链存证，一旦出现交易纠纷、可疑资金行为，

监管核查、司法取证缺少完整可信凭证。四是安全技术落地标准不统一，国密算法应用、数据隔离、接口鉴权、异常事务回滚缺少统一要求，部分系统明文传输敏感报文、本地存储用户钱包私钥与身份隐私，存在数据泄露、中间人攻击、重放攻击等安全隐患。五是业务流程缺少标准化定义，用户委托自动支付、人工确认支付、智能体间付费交互、数字人民币智能合约履约支付、大额人工审批等典型场景流程碎片化，不同服务商业务逻辑不一致，监管缺少统一核查依据。

与此同时，苏州作为全国数字人民币综合试点城市，已建成成熟的苏州市金融服务多智能体协作网络，在多智能体调度、数币对接、区块链存证、分级风控等方面形成完整工程实践，具备将落地经验转化为标准化文件的实践基础。

（二）立项意义

1.填补国内标准空白，完善数字人民币创新应用标准体系。目前国内现有数字人民币相关标准多聚焦基础支付、智能合约、钱包运营单一维度，缺少面向多智能体自动化交易场景的综合性技术规范，本标准首次完整定义智能体交易全链路技术、安全、流程、集成要求，补齐细分领域标准短板，完善数字人民币行业标准框架。

2.筑牢用户资金与隐私安全防线，强化金融风险防控。通过双层授权模型、九项额度与主体强制校验、全流程区块链存证、国密全链路加密、数据不出域等强制性条款，从架

构底层约束智能体越权操作、伪造支付行为，实现每一笔自动化交易可授权、可校验、可追溯、可拦截，有效防范资金挪用、电信诈骗、隐私泄露等金融风险。

3.降低行业数字化建设成本，推动技术生态兼容互通。标准统一存量平台接入式集成方案，明确模块化、热插拔MCP工具开发规范，统一对外接口报文、加密、鉴权标准，减少机构重复研发投入，打通不同厂商智能体系统互通壁垒，构建开放兼容的数字人民币智能体产业生态。

4.赋能监管数字化治理，提升监管核查效能。标准统一交易流水、授权凭证、存证数据、审计报表标准化格式，建立标准化监管查询接口，监管机构可依托统一规范快速完成交易溯源、可疑资金排查、合规审查，解决以往数据标准不一、取证困难、核查效率低的监管痛点。

5.支撑数字经济与实体经济深度融合，服务国家数字人民币推广战略。标准化智能体自动交易能力可广泛应用于租赁采购、供应链履约、公共服务自动扣费、跨智能体有偿服务等场景，提升实体经济数字化支付效率，将苏州试点成熟模式标准化输出，为全国各试点城市落地同类创新场景提供规范指引，助力数字人民币常态化、规模化应用。

6.落实数据安全、个人信息保护、反洗钱相关法律法规要求。标准将《数据安全法》《个人信息保护法》《数字人民币试点管理办法》等监管要求转化为可落地技术条款，明

确敏感数据存储、传输、使用约束，完善大额、可疑交易监测处置机制，保障智能体交易业务全流程合法合规

二、本标准适用范围及概要

（一）适用范围

本标准适用于面向个人用户、企事业单位、个体工商户等市场主体建设与运营的数字人民币多智能体自动化交易系统，覆盖系统架构设计、智能体开发、授权凭证管理、交易流程设计、安全体系搭建、存量平台集成复用、项目实施测试、运维监控、合规审计全环节。

标准约束对象包含系统开发服务商、数字人民币智能体平台运营机构、接入平台的商户与企业用户、提供区块链存证、身份核验、智能合约配套服务的第三方技术机构；同时可供金融监管机构、标准化评审单位开展系统合规评估、项目验收时参考使用。

本标准仅针对数字人民币多智能体自动化交易场景技术规范，不替代央行数字人民币基础支付、智能合约官方接口规范，系统对接官方数币平台仍需同步遵循人民银行发布的系列官方标准。

（二）标准概要

本标准按照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》编制，全文共11个核心章节，配套前言、规范性引用文件、术语定义内容，整体分为五大

逻辑板块：

第一板块为基础总则（第1章至第4章），明确标准适用边界、规范性引用文件、数字人民币智能体核心术语定义，提出合规性、公平性、安全性、可持续性、可追溯五个基本原则，详细规定四层四域兼容ACT协议系统总体架构，逐层拆解用户入口层、多智能体协作层、服务与工具层、对接层功能模块、技术约束与设计要求，明确OrchClaw编排引擎、授权Agent、交易Agent、支付Agent、存证Agent四个核心智能体能力规范。

第二板块为业务流程与授权凭证核心技术要求（第5章、第6章），标准化S1用户委托支付、S2用户确认支付、S3智能体间支付、S4数币智能合约支付、L3大额人工审批五个核心业务全流程；构建二级授权模型，完整定义支付委托书、支付令牌标准字段、SM2签名防伪规则、支付前九项强制校验逻辑，规范两类凭证完整生命周期管理、归档留存年限要求。

第三板块为全维度安全体系规范（第7章），从通信安全、授权安全、大额风险管控、身份认证、审计存证、异常容错、数据安全七大维度制定强制性安全条款，统一SM4传输加密、双向TLS鉴权、权限物理隔离、区块链全节点上链、数据不出域、事务自动回滚等落地细则。

第四板块为存量系统集成复用与项目实施验收（第8章、

第9章），明确苏州市金融服务多智能体协作网络存量组件接入式复用总则，分别对编排引擎、MCP工具层、智能体信息广场、区块链存证、基础权限框架复用划定改造边界；制定12个月五阶段实施计划，统一功能、性能、安全三类测试用例设计标准与量化验收指标。

第五板块为运营运维与合规档案管理（第10章、第11章），规范7×24小时值守日常运维、全维度实时监控、多场景应急处置、五级分类日志管理要求；明确金融合规管控细则、业务与技术档案归档、保管、销毁全流程管理标准。

三、国内外相关标准情况

（一）国际相关标准现状

国际范围内暂无针对数字人民币多智能体自动化交易的专项技术标准，相关规范分散在人工智能多智能体框架、通用数字货币支付、网络安全、区块链存证领域通用标准中，且无法适配我国数字人民币监管体系、人防与实体经济融合场景、国密算法国产化安全要求，可借鉴价值有限。

1.多智能体领域：国际标准化组织ISO、IEEE发布多智能体协同、任务调度通用框架标准，侧重通用AI程序通信逻辑，未结合金融支付场景设置资金授权、额度风控、交易存证约束，不具备金融业务适配性。

2.数字货币支付领域：欧美稳定币相关技术规范仅围绕加密资产转账、钱包交互设计，缺少法定数字货币监管账户、

智能合约履约、分级人工审批等合规机制，与数字人民币法定货币属性、监管框架存在本质差异。

3. 安全与区块链领域：国际通用区块链、传输安全标准以RSA、ECC国际加密算法为核心，未纳入我国GM/T 0002 SM4、GM/T 0003 SM2国密算法体系，无法满足国内金融行业国产化密码应用强制要求。

4. 行业应用层面：欧美、日韩车辆租赁、供应链自动化支付规范以企业自律条款为主，无公共资金监管、多层授权、智能体自动交易融合规范，不存在与本标准匹配的综合性行业标准，无成熟国际范本可直接引进转化。

（二）国内相关标准现状

国内现有标准分为数字人民币基础标准、人工智能标准、金融安全标准、区块链存证标准、车辆租赁行业标准五大类，均为单一领域专项规范，缺少融合多智能体自动化交易的综合性技术标准，存在标准空白：

1. 数字人民币相关标准：央行及金标委发布数字人民币钱包、支付接口、智能合约、监管账户基础规范，仅定义基础转账、合约部署底层接口，未覆盖多智能体自主交易、分层授权、智能体调度、跨Agent付费场景技术要求，无法支撑自动化交易场景落地。

2. 人工智能多智能体标准：全国信标委发布多智能体系统通用架构、协同交互标准，聚焦通用AI技术，未结合金融

资金交易增加风控、授权、资金追溯强制性条款，金融场景适配性不足。

3.金融与密码安全标准：GM/T系列国密标准、金融数据安全、支付系统安全规范明确加密、数据分级、接口安全通用要求，但未针对智能体双层授权、令牌防伪、交易全链路存证制定细分落地细则。

4.区块链存证标准：司法、金融区块链存证标准规定数据上链、哈希核验通用流程，未匹配数字人民币智能体交易多节点存证、监管专项查询台账等特色需求。

5.车辆租赁等行业团体标准：现有租赁行业规范聚焦线下合同、线下资金监管，未融合AI智能体自动交易、数币智能合约、跨智能体付费数字化新模式。

综上，国内暂无覆盖系统架构、智能体开发、双层授权、标准化交易流程、存量平台集成、全链路安全、项目实施运维的数字人民币智能体交易综合技术规范，制定本标准能够有效填补细分领域标准空白，形成国内首创、适配本土监管与技术体系的团体标准。

四、标准编制原则和主要技术内容确定的依据

（一）标准编制原则

1.合规优先原则

标准全部条款严格对标《数字人民币试点管理办法》《数据安全法》《个人信息保护法》《人民币银行结算账户管理

办法》GM/T国密系列标准、GB/T 1.1标准化导则等国家法律法规、行业监管文件，所有技术设计、流程规则、安全要求均满足金融反洗钱、消费者权益保护、密码应用合规硬性要求，不出现与现行监管规则冲突的内容。

2.实用性与落地性原则

标准全部技术内容基于苏州已落地运行的金融多智能体协作网络、数字人民币智慧监管平台真实工程实践提炼，架构设计、智能体功能、业务流程、集成复用方案均经过线上业务验证，量化性能指标、测试方案、运维流程贴合中小机构、大型平台不同规模主体建设需求，可直接指导项目开发、验收、运营，杜绝脱离实际的理想化技术条款。

3.兼容性与复用性原则

标准确立接入式集成改造思路，充分复用存量金融多智能体平台底层能力，不强制重构现有系统；统一接口、报文、加密、智能体通信通用规范，兼容不同厂商开发的智能体模块、MCP 工具，保障新旧系统、跨厂商组件互联互通，降低行业改造成本。

4.安全底线刚性约束原则

将资金安全、隐私保护、交易可追溯作为强制性核心要求，双层授权模型、九项支付校验、国密全链路加密、数据不出域、区块链全节点存证、大额人工审批等关键安全条款设置为硬性规范，不允许系统开发方删减、绕过相关校验逻

辑，从标准层面封堵安全漏洞。

5.分层分级、权责隔离原则

系统架构、智能体职责、权限管控、风险处置全程落实隔离设计，授权、交易、支付、存证智能体逻辑完全分离；权限分为L1/L2/L3三级，大额、高风险交易强制人工介入，实现操作权责分离、风险分级管控。

6.可追溯可审计原则

标准要求交易、授权、配置变更、运维操作全节点留痕上链，统一数据格式、归档年限、审计报表规范，配套标准化监管查询接口，满足内部审计、监管核查、司法取证全流程溯源需求。

7.适度前瞻性原则

在满足当前数字人民币试点业务需求基础上，兼容智能体规模化协同、跨场景智能合约、多维度风控模型迭代等未来业务拓展需求，架构采用模块化、热插拔设计，预留功能扩展接口，保障标准中长期适用性。

（二）主要技术内容确定依据

1.系统四层四域架构、OrchClaw编排引擎、四类核心智能体设计依据：苏州市金融服务多智能体协作网络现有成熟落地架构，结合多智能体ACT通用通信协议、金融分布式系统高可用设计规范，参考分布式交易系统高内聚、低耦合通用设计理论，经多轮内部技术评审、行业专家论证确定层级

划分与模块职责。

2. 二级授权模型、支付委托书与支付令牌全套规范依据：数字人民币资金监管、用户授权管理相关监管指引，结合金融支付行业“长期授权+单次凭证”双重风控成熟实践，基于SM2国密数字签名防伪技术规范，针对智能体无人自动交易场景优化额度黑白名单、收款方约束、时效管控细分字段。

3. 五大标准化交易业务流程依据：苏州数字人民币智能体采购、自动履约、跨AI服务付费、智能合约分账真实业务场景，梳理用户自主委托、人工确认、智能体交互、合约触发、大额风控五类高频业务全链路节点，结合反洗钱可疑交易识别、消费者权益保护要求补充告警、回滚、人工审批分支流程。

4. 全维度安全体系条款依据：GM/T 0002、GM/T 0003国密密码应用规范，金融信息系统等级保护2.0要求，《个人信息保护法》敏感数据不出域、最小权限原则，区块链司法存证不可篡改规范，分布式系统熔断、容错、事务一致性技术标准。

5. 存量平台集成复用规范依据：现有苏州金融多智能体网络运行改造实践，兼顾存量系统稳定运行与新增数币业务独立隔离需求，参考金融系统平滑升级、灰度发布工程实施标准，明确复用边界与新增模块隔离规则。

6.分阶段实施、测试验收量化指标依据：金融数字化项目标准实施周期、分布式交易系统通用性能基准、支付系统安全渗透测试行业标准，结合数字人民币交易并发、时延、上链效率真实运行数据，设定可量化、可落地的验收阈值。

7.运维监控、应急处置、合规档案条款依据：金融机构7×24小时运维管理规范、支付系统应急预案指引、金融业务档案保管年限监管要求、反洗钱定期审计报告制度

五、技术保障及工作进度计划

（一）技术保障

1.平台实践支撑保障

依托江苏金服数字集团已建成运营的苏州市金融服务多智能体协作网络、数字人民币智慧监管平台，拥有完整多智能体调度、数币支付对接、区块链存证、智能合约落地案例，可提供真实场景数据、系统原型、测试环境支撑标准条款验证，确保技术内容具备落地实践支撑。

2.跨领域专家团队保障

组建由数字人民币技术专家、国密密码安全专家、多智能体AI研发工程师、金融风控合规专家、标准化评审专家、行业商户与保险机构业务代表构成的编制专家组，覆盖技术、合规、业务、标准全链条，全程参与条款论证、试验验证、意见评审，保障标准科学性、严谨性。

3.政策与合规技术支撑

深度对接地方金融监管、人民银行数字人民币试点管理部门，同步跟踪数字人民币最新监管政策，所有条款开展合规前置审查，避免出现监管冲突；联合密码机构开展国密算法落地测试，验证加密、签名、验签全流程安全性与性能。

4.测试与验证技术保障

搭建独立数字人民币沙箱测试环境、多智能体仿真压力测试平台，针对标准架构、授权模型、交易流程、安全规范开展全场景功能、压力、渗透测试，所有量化性能指标均通过实测校验，确保指标合理可行。

5.产学研协同保障

联合集团人工智能子公司、金服实验室科技公司开展智能体前沿技术研究，同步联动车辆租赁、供应链、公共服务行业龙头企业收集业务痛点，吸纳产业一线实操经验完善标准内容。

（二）工作进度计划

1.启动阶段（2026年6月）：完成国内外数字人民币、多智能体、金融安全、区块链相关标准全面梳理，检索ISO、国标、行标、现有团体标准；搭建标准指标体系初稿，完成架构、授权、流程、安全四大维度指标、定义初步编制；同步完成立项申报材料撰写；

2.调研阶段（2026年8月）：针对初步构建的指标体系，向相关主体发放调研问卷，收集对指标选取、定义、数据来源等方面的意见。

六、其他需要说明的内容

无。