《金融服务多智能体协作网络技术规范》
团体标准编制说明

一、立项的意义

随着大模型技术迭代升级，多智能体（Multi-agent）协作成为人工智能产业发展核心方向，AI从单一工具向“协同工作体”跨越，为金融行业数字化转型提供关键技术支撑。金融行业兼具数据密集、流程复杂、合规严格、风险敏感等特性，是多智能体技术落地的核心场景，但其跨机构协作长期面临数据孤岛、审批冗长、合规滞后、风控薄弱、标准缺失五大痛点。

当前我国金融服务多智能体应用处于试点探索阶段，技术架构、协作机制、安全规范、运营体系均无统一标准，导致行业出现技术碎片化、应用孤岛化、风险不可控、合规无依据等问题。为破解行业痛点、规范技术应用、筑牢安全防线、推动产业规模化发展，亟需制定团体标准，明确金融服务多智能体协作网络的技术框架、核心要求、安全准则与运营规范。

本标准立项，一是填补国内空白，构建国内首个金融领域多智能体协作技术标准，终结行业无标可依的局面，提升我国金融科技标准话语权；二是规范技术应用，统一架构、接口、行为、安全要求，降低跨机构协作成本，避免无序发展；三是保障合规安全，贴合金融监管要求，明确权限、审

计、风控、合规规则，防范技术应用风险；四是赋能实体经济，优化融资流程、提升服务效率，缓解中小企业融资难题；五是引领产业发展，形成可复制推广的“苏州模式”，推动金融科技自主可控、高质量发展，助力数字经济建设。

二、本标准适用范围及概要

（一）适用范围

本标准适用于金融机构、金融科技企业、监管机构及相关服务提供方，涵盖银行、证券、保险、资产管理、征信、支付等领域，用于金融服务多智能体协作网络的规划、设计、研发、部署、接入、运维、评测、合规管理全流程。

标准适用场景包括：企业授信融资、风控审核、合规审查、资金支付、监管报送、数字人民币应用、贷后管理、投研辅助等跨机构、跨系统、跨业务的多智能协作场景，为相关系统建设、技术选型、合规校验、质量评测提供统一技术依据与合规参考。

（二）概要

本标准属于金融科技领域基础通用性团体标准，核心围绕“多智能体协作网络”，构建“七层架构、四大核心、三大机制、一套安全、一套运营”的完整技术体系，全文共11章，核心内容概要如下：

范围、规范性引用文件、术语和定义：明确标准适用边界、引用基础标准，界定智能体、多智能体协作网络、编排

引擎、智能体信息共享广场等核心术语，统一行业认知。

总体架构：规定编排层、业务层、信息共享层、工具层、接入层、安全层、运营层七层架构，明确各层功能定位、核心模块及交互逻辑，构建完整技术栈。

智能体行为框架要求：明确身份立场文件、分区记忆系统、主动触发机制三大核心要素，规范智能体角色、记忆管理、主动行为规则，确保行为可控、可解释、可审计。

多智能体协作编排要求：规定全局编排引擎能力，明确授信、风控、合规、支付四类核心业务智能体的功能、技能及协作规则，支撑跨任务并行调度与结果仲裁。

信息共享和协作机制：规范智能体实时信息共享广场、组织知识共享广场建设要求，明确事件广播、评论协作、知识管理规则，保障跨智能体、跨机构信息安全高效流转。

工具层（MCP）要求：明确征信、工商、纳税、反洗钱、黑名单、大额报送、数字人民币、区块链存证、身份核验、市场利率10类核心金融工具的标准化封装、鉴权、限流、审计要求。

安全接入和内网对接：规定网关接入层架构、轮询模式、适配规范及安全防护要求，确保金融机构内网数据不出域、安全接入。

权限分级和安全体系：建立L1/L2/L3三级权限分级体系，明确身份认证、访问控制、安全威胁防御要求，筑牢金融级

安全防线。

智能体评测和持续运营要求：规定DMHR动态多维评测方法、自动化评测、专家评审、版本管理、故障响应、运营监控要求，保障网络稳定可靠、持续迭代。

三、国内外相关标准情况

（一）国际相关标准现状

国际上多智能体技术研究起步较早，但尚未形成金融领域专用技术标准，相关标准集中于通用AI、大模型、通用智能体通信等领域，无针对性金融场景规范。

通用智能体标准：国际标准化组织（ISO）、电气和电子工程师协会（IEEE）发布少量AI通用标准，聚焦智能体基础定义、通信协议、安全框架，如A2A、MCP协议，但缺乏金融合规、数据安全、风控联动、审计追溯、权限分级等金融级特殊要求，无法适配金融行业强监管、高风险特性。

金融科技标准：国际金融稳定委员会（FSB）、巴塞尔委员会发布金融科技相关指引，侧重AI风控、数据治理、合规管理，但未涉及多智能体协作网络架构、编排、信息共享、接入适配等核心内容，无跨机构协作技术规范。

应用现状：国际金融机构多为单点试点多智能体应用，无规模化跨机构协作网络，技术方案碎片化、无统一框架，无法形成行业共识，国际标准处于空白状态，为我国自主制定标准提供窗口期。

（二）国内相关标准现状

国内金融科技标准体系逐步完善，但金融服务多智能体协作网络相关国家标准、行业标准、团体标准均为空白，现有标准无法覆盖跨机构多智能体协作核心场景。

通用AI标准：发布《人工智能安全治理规范》《生成式人工智能服务安全基本要求》等标准，聚焦AI基础安全、伦理规范，未针对金融场景定制，无多智能体协作相关内容。

金融科技基础标准：发布《金融数据安全数据生命周期安全规范》《商业银行人工智能技术应用指引》等标准，侧重单一机构内部AI应用、数据治理、风控合规，未涉及跨机构协作、全局编排、智能体行为治理、信息共享、接入适配等核心内容。

智能体相关探索：国内部分企业开展智能体技术研发与试点，但均为企业内部标准或技术文档，未形成行业统一规范，存在架构不一、接口不兼容、安全标准各异等问题，制约行业规模化落地。

综上，国内外均无针对金融服务多智能体协作网络的专用标准，本标准制定填补行业空白，契合我国金融科技发展需求，具备行业引领性与前瞻性。

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

合规优先，底线思维：严格遵循《中华人民共和国网络

安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《金融科技发展规划（2022—2025年）》等法律法规与监管要求，贴合金融行业合规底线，确保标准内容合法合规、符合监管导向。

安全可控，风险闭环：立足金融高风险特性，坚持数据不出域、权限最小化、全链路审计、风险可追溯，构建从接入、传输、存储、调用、决策到运营的全流程安全体系，防范技术应用风险，保障金融数据与业务安全。

实用可行，贴合实际：聚焦金融行业核心痛点与实际业务需求，立足苏州试点实践经验，不追求过度超前、不脱离行业现状，技术要求兼顾先进性与落地性，确保金融机构、科技企业可落地、可执行、可推广。

开放兼容，生态共建：兼容主流技术框架、接口协议与行业实践，支持异构智能体、异构系统接入，不设置技术壁垒、不绑定特定产品，为行业生态共建提供开放标准，推动产业链协同发展。

自主创新，引领发展：基于我国金融行业特性与技术实践，提炼自主可控的技术体系，突出中国特色、自主创新，避免照搬国际标准，提升我国金融科技标准话语权，引领行业高质量发展。

系统完整，逻辑严谨：标准结构科学、逻辑清晰、内容全面，覆盖多智能体协作网络全生命周期，术语统一、表述

规范、要求明确，具备系统性、完整性、严谨性，便于行业理解与执行。

（二）主要技术内容确定的依据

本标准核心技术内容，以行业痛点、监管要求、试点实践、技术成熟度为核心依据，结合国内外技术趋势，经调研论证、专家研讨、试点验证后确定，具体如下：

总体架构：依据金融跨机构协作“多主体、多系统、高安全、强协同”特性，结合OpenClaw框架试点实践，构建七层架构，覆盖从底层接入到上层运营的全链路，解决架构混乱、层级不清、功能重叠问题，确保架构科学、分工明确、协同高效。

智能体行为框架：依据智能体“身份、记忆、主动行为”核心特性，结合金融合规、风控要求，确定SOUL、MEMORY、HEARTBEAT三大要素，解决智能体行为不可控、经验不可沉淀、无主动感知问题，确保智能体行为合规、可解释、可追溯。

多智能体协作编排：依据金融业务“并行任务、结果仲裁、分级审批”需求，结合OrchClaw引擎试点经验，明确编排引擎与四类核心智能体要求，解决任务拆分混乱、调度低效、决策冲突问题，支撑复杂业务高效协同。

信息共享和协作机制：依据金融跨机构“实时联动、知识统一、安全流转”需求，结合试点中风险联动、合规同步

痛点，确定实时共享广场与知识共享广场要求，解决信息孤岛、同步滞后、知识碎片化问题，保障信息高效流转。

工具层（MCP）：依据金融业务高频工具需求，结合征信、反洗钱、数字人民币等场景实践，筛选10类核心金融工具，解决工具接口不统一、调用无规范、审计不完整问题，实现工具标准化调用。

安全接入和内网对接：依据金融“数据不出域、内网安全”核心要求，结合Gateway试点实践，确定接入架构、适配规范与安全防护要求，解决跨机构数据泄露、内网暴露风险，筑牢数据安全防线。

权限分级和安全体系：依据金融风险分级管理要求，结合监管审批规则，建立L1/L2/L3三级权限体系，明确安全防护要求，解决权限滥用、决策失控、安全攻击问题，构建金融级安全屏障。

智能体评测和持续运营：依据AI系统质量管控要求，结合试点运营痛点，确定DMHR评测方法与运营规范，解决质量不可控、迭代无依据、故障无响应问题，保障网络持续稳定、高质量运行。

五、技术保障及工作进度计划

（一）技术保障

牵头单位技术支撑：江苏金服数字集团有限公司作为牵头单位，具备扎实技术积累，自主研发OpenClaw智能体协作

框架、OrchClaw全局编排引擎、四类核心业务智能体、智能体信息共享广场、Gateway接入层、DMHR评测平台等核心技术，核心指标经试点验证，技术成熟、稳定可靠，为标准编制提供核心技术支撑。

产学研协同支撑：联合苏州银行、东吴证券、东吴财险、苏州资管、工行苏州分行等金融机构，提供业务场景、合规经验、行业需求支撑；联合上交大苏州创新院等高校，提供理论研究、技术指导、前沿趋势支撑；组建标准化专家团队，提供标准框架、语言规范、合规审核支撑，形成产学研用协同的技术保障体系。

试点实践支撑：依托苏州市金融服务多智能体协作网络创新联合体试点成果，已接入多家金融机构，落地中小企业融资、数字人民币支付、监管报送等场景，积累丰富实践数据、案例、经验，为标准内容验证、优化提供实践支撑，确保标准贴合实际、可落地。

调研论证支撑：编制组将开展多轮行业调研，2026年4月赴苏州、深圳试点地区实地走访金融机构、监管部门、中小企业，发放调研问卷，广泛收集行业意见；组织多轮专家研讨，邀请金融、科技、合规、标准化专家论证标准内容，确保标准科学合理、贴合行业需求。

（二）工作进度计划

1.启动阶段（2026年2月）：完成文献调研、国内外标准梳理，召开编制启动会，明确分工与技术路线；形成指标体系初稿，包含维度划分、指标清单及初步定义；

2.调研阶段（2026年4月）：开展实地调研，收集政府部门、金融机构、企业的意见；针对初步构建框架，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。

3.立项阶段（2026年8月）：将编制好的标准发给商会，进行专家立项评审，根据立项评审意见修改文本。

六、其他需要说明的内容

无。