ICS 03.060
CCS A 11

T/SZFCC

苏州市金融业商会团体标准

T/SZFCC XXXX—XXXX

AI 智付-数字人民币城市智能体互联网数字消费场景应用技术规范

AI intelligent payment—Technical specification for application of e-CNY city agent internet in digital consumption scenarios

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

苏州市金融业商会　　发 布

目　　次

前言 II
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　总体架构 2
5.1　总体原则 2
5.2　七层技术架构 2
6　核心技术要求 4
6.1　智能体互联网底座 4
6.2　大语言模型能力 5
6.3　商户智能体 5
6.4　数字人民币智能支付 6
6.5　MCP 接入要求 6
7　数字消费场景要求 6
7.1　线下商圈消费 6
7.2　线上商城消费 6
7.3　生活缴费 7
7.4　文旅/景区消费 7
7.5　预付费消费 7
8　安全与合规 7
8.1　数据安全 7
8.2　交易安全 8
8.3　合规要求 8
8.4　交易风险下各方权责划分 8
9　运维与应急 8
9.1　日常运维 8
9.2　应急处置 9

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。

本文件由江苏金服数字集团人工智能科技有限公司提出。

本文件由苏州市金融业商会归口。

本文件起草单位：江苏金服数字集团有限公司、江苏金服数字集团人工智能科技有限公司、上交大苏州创新院、东吴证券股份有限公司、苏州东吴财产保险股份有限公司、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、周军、孔淳、梁媛、唐淑艳、张子华、施爱博、马骏俊、章国新、李庆坤、吴李沅、李豪奇、宋豪、周凡、谢婷婷、李宁。

AI 智付-数字人民币城市智能体互联网数字消费场景应用技术规范

1 范围

本标准规定数字人民币城市智能体互联网（AI智付）在数字消费场景的总体架构、核心技术要求、数字消费场景要求、安全与合规、运维与应急等要求。

本文件适用于政府监管机构、金融机构、支付机构、商圈运营方、商户、智能体开发方、技术服务商在数字消费场景开展AI Agent+数字人民币融合应用的设计、开发、部署、测试、运维与监管。

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 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 35273—2020 信息安全技术 个人信息安全规范
GB/T 42571—2023 信息安全技术 区块链信息服务安全规范
GB/T 45654—2025 网络安全技术 生成式人工智能服务安全基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

AI 智付 AI intelligent payment

以城市智能体互联网为底座、大语言模型为核心、数字人民币智能合约为支付载体,实现意图解析、智能撮合、自动履约、合规清算的新一代智能支付体系。

3.2

数字人民币城市智能体互联网 e-CNY City agent internet

面向城市数字消费，以数字人民币为价值载体、以智能体互联协议为通信底座、以全局编排为协同核心，实现人—智能体—商户—金融机构可信互联、任务自治、价值流转的分布式智能网络。

3.3

消费智能体 consumer agent

具备SOUL身份、MEMORY记忆、HEARTBEAT主动触发，可完成消费推荐、订单生成、合规校验、数字人民币支付、售后协同的专用智能体。

3.4

AI 智付交易 AI intelligent payment transaction

由智能体在用户授权范围内，自主发起/协助完成的数字人民币消费支付、退款、核销、合约执行等交易。

4 缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）
ACT：智能体通信工具集（Agent Communication Toolkit）
e-CNY：数字人民币（Digital Currency Electronic Payment）
MCP：智能体标准通信协议（Model Context Protocol）
REST：表述性状态转移（Representational State Transfer）
API Key：应用程序接口密钥（Application Programming Interface Key）

5 总体架构

5.1 总体原则

5.1.1 安全可控

坚守金融业务安全底线，建立覆盖消费业务全流程、全参与主体、全业务环节的安全保障机制，实现业务权限可管控、业务行为可核查、业务交易可追溯。业务相关信息宜在受控安全域内开展处理，确需对外提供信息的，应当符合法律法规及监管制度要求，切实保障消费者、商户、金融机构的信息与交易安全。

5.1.2 自主协同

以智能体承担业务办理为主要方式，实现多方业务主体协同配合、业务事件联动响应、消费事项自动分解与推进，推动数字消费服务由人工逐项办理模式，转变为“多智能体协同办理+关键业务节点人工确认”的新型业务服务模式。

5.1.3 标准开放

应遵循统一的智能体身份识别、业务交互、业务能力调用、服务质量评价业务规则，支持不同平台、不同业务生态、不同机构的智能体之间相互识别、协同开展消费业务，实现跨生态业务互通。

5.1.4 合规先行

将反洗钱、反欺诈、大额业务报送、消费者权益保护相关要求融入消费业务全过程，落实参与主体资质核查、业务风险动态管控、业务信息报送、全业务链条留痕核查等工作，确保各项业务开展符合监管规定。

5.1.5 便民利企

面向消费者优化消费交互体验，支持无感支付、简化业务操作流程；面向中小商户降低接入实施门槛，支持商户零代码创建智能体，减少技术改造成本，提升商户运营效率，兼顾消费者便利与中小市场主体发展需求。

5.1.6 可扩展可持续

业务运行模式具备良好的兼容拓展能力，能够适配新增消费场景与新型业务服务；建立标准迭代更新机制，跟随智能体应用模式、数字人民币业务模式的发展持续优化，保障本标准能够长期指导数字消费业务开展。

5.2 七层技术架构

5.2.1 总体架构

5.2.1.1 采用七层一体化技术架构，自下而上依次为全局编排引擎层、核心业务智能体层、实时信息共享广场层、标准化工具层、安全接入层、权限分级与安全体系层、评测与运营体系层。

5.2.1.2 各层解耦协同，围绕数字人民币数字消费业务，形成从业务任务协同、消费业务执行、信息互通、外部业务能力调用、系统安全接入、风险权限管控到服务质量运营评估的完整业务支撑体系。

5.2.2 全局编排引擎层

5.2.2.1 面向消费全流程，实现各类消费相关业务任务的统一统筹协同，支撑消费业务任务拆解、多参与方业务并行协作、业务冲突处置、业务状态统一管理、业务执行模式判定。

5.2.2.2 应具备业务任务拆解、多方业务并行协同、业务冲突仲裁、分级权限管控、高风险大额业务挂起、业务行为审计留痕能力，统筹消费、支付、风险防控、合规校验四类业务智能体协同开展数字消费业务。

5.2.2.3 应展多方业务协同过程中，应防范多业务并行处理带来的业务数据状态不一致问题，具体要求如下：

a) 核心业务数据表读写锁控制：针对订单、支付、用户授权、业务合约等关键业务数据，业务协同能力应具备读写锁管控能力；会变更业务状态的业务操作采用排他锁；查询类读取操作可采用共享锁；存在未办结业务事务时，阻断相冲突的业务变更请求，避免多方并发操作造成业务数据错乱；
b) 跨业务智能体并发的数据一致性校验：消费、支付、风控、合规业务智能体同步开展业务处理时，应对订单状态、支付结果、风险标记、合规标识等关键业务字段开展一致性核验；一旦发现业务数据视图不一致，立即启动业务冲突处置，终止后续业务流转并留存完整异常审计记录；
c) 业务事务与异常处置：一组相互关联的多智能体协同业务应当支持事务化处理；部分业务环节执行异常时，按照业务规则完成业务状态回滚或者异常隔离，避免产生无效业务数据。

5.2.3 核心业务智能体层

5.2.3.1 应承载数字消费全流程各类业务角色能力，由消费智能体、商户智能体、智付智能体、风控智能体、合规智能体共同组成，承担数字消费业务全流程业务办理工作：
a) 消费智能体：理解用户消费诉求，匹配商户资源，生成消费订单，协助发起数字人民币支付业务；
b) 商户智能体：负责商户商品服务管理、接收消费订单、同步履约进展、开展售后业务协同；
c) 智付智能体：办理数字人民币支付业务、执行智能合约分账清算、处理退款相关业务；
d) 风控智能体：开展交易风险识别、黑名单管理、交易集中度核查、风险预警提示；
e) 合规智能体：开展业务资质核验、触发业务报送、同步监管规则、校验业务用途合规性。
5.2.3.2 各类业务智能体具备对应业务处理能力，可独立完成细分业务事项，并在全局业务协同下配合完成完整数字消费业务。

5.2.4 实时信息共享广场层

5.2.4.1 实时信息共享广场层应面向数字消费参与各方，实现业务事件广播、业务消息实时传递、业务主体间业务协同沟通以及业务公共知识共享。
5.2.4.2 应能够同步风险提示、合规新规、订单进度、支付结果、履约状态等业务信息；汇集监管规则、数字人民币业务要求、商圈经营规则、历史业务参考案例，为各业务智能体开展业务处置提供统一业务依据。

5.2.5 MCP 标准化工具层

5.2.5.1 MCP 标准化工具层应对数字人民币支付、身份核验、资质核查、黑名单校验、反洗钱核查、大额业务报送、业务存证、订单履约、退款核销等高频消费相关业务能力做标准化封装。
5.2.5.2 通过统一身份核验、业务流量保护、结果复用、业务调用审计等机制，屏蔽外部机构业务系统差异，让业务智能体可以安全、可控地调用外部业务能力。面向大量商户、机构存量异构业务系统接入场景，应具备多端业务接口自动适配与校验能力，具体要求如下：
a) 业务接口文档解析：可读取商户、合作机构提供的业务接口说明，识别业务字段、请求内容、返回结果、异常业务编码，自动获取业务接口信息；
b) 非标业务接口适配：对于字段、格式不统一的存量外部业务接口，支持字段映射、格式转换、数据适配，把外部非标业务接口转换为本标准统一业务能力模型，降低合作机构系统改造工作量；
c) 业务接口自动校验：对外部传入参数、返回业务数据、业务取值范围开展校验；校验不通过的阻断业务调用，留存清晰异常记录；
d) 适配规则版本管理：接口适配、字段映射规则支持版本留存、变更留痕、版本回退，适配外部合作机构业务迭代调整。

5.2.6 安全网关安全接入层

5.2.6.1 负责银行、支付机构、商圈收银、商户系统、监管节点等各类业务参与方的业务接入。采用内网主动获取业务信息、外部网络不直接连通内网的业务部署模式，保障业务数据安全。
5.2.6.2 应为各业务参与方提供安全业务通路、业务信息脱敏、异常业务行为识别、全流程业务操作审计等业务保障能力。

5.2.7 权限分级与安全体系层

5.2.7.1 本层落实数字消费全流程业务风险管控，建立 L1 自主处理、L2 消息告知、L3 人工审批三级业务处置权限。L3 级大额业务、高风险业务必须经过人工审批后方可继续办理，内容如下：

a) 大额业务处置门槛：本标准设置大额业务最低管控底线，实施主体可在不低于该底线基础上，结合业务场景、用户风险等级、属地监管要求，设定机构自身大额业务触发门槛；门槛配置、调整记录应当归档留存，接受审计核查；

b) L3 高风险业务包括但不限于：跨境支付业务、预付费专户资金提取业务、批量退款业务、批量合约变更业务、用户限额调整业务、批量授权变更业务；实施主体可结合自身业务风险补充扩展高风险业务清单。

5.2.7.2 应落实智能体身份核验、基于角色的访问权限管控、业务最小权限分配、恶意提示风险防范、业务行为基线监测、高敏感业务二次确认等安全业务机制，防范越权办理业务、恶意业务注入、业务信息泄露、业务交易被篡改等各类业务风险。

5.2.8 评审评测与运营体系层

5.2.8.1 评审评测与运营体系层承担智能体服务质量评估与业务运营保障工作，采用大模型辅助评估结合金融专家评审的方式，围绕业务结果准确性、业务合规水平、风险处置能力、业务办理时效、业务可解释性、业务运行稳定性，对智能体业务服务质量开展评估。

5.2.8.2 应提供智能体服务准入、服务降级、服务退出、版本管理、业务故障处置、业务运行监控等运营保障能力，保障数字消费相关智能体业务持续稳定对外提供服务。

6 核心技术要求

6.1 智能体互联网底座

6.1.1 支持全局唯一身份注册、语义发现、路由寻址、跨生态互通，要求如下：

a) 为每个接入智能体分配全局唯一、不可篡改、全生命周期可追溯的智能体 ID，身份信息包含机构主体、服务类型、能力标签、接入资质、有效期、数字证书等核心要素，确保跨平台、跨机构、跨生态唯一识别；

b) 提供语义级智能发现能力，基于用户意图、服务标签、能力特征、地理位置、服务范围进行精准匹配，支持模糊意图、场景化需求下的智能体精准检索；

c) 具备多级路由寻址能力，支持城域网、区域网、全国网分层调度，可按地域、业态、能力优先级动态路由，保障高并发、跨区域场景下的调度效率；

d) 支持跨生态互通互认，兼容开放原子、阿里 ACT、行业联盟等主流智能生态，实现异构智能体身份互认、服务互通、数据可信交互，打破生态壁垒。

6.1.2 应兼容 MCP+ACT 协议，支持异构智能体接入，具体要求如下：

a) 全面兼容 MCP 标准通信协议，支持流式传输模式、标准输入输出模式、开放应用程序接口模式三种接入模式，适配实时、命令行、REST 各类异构智能体；

b) 兼容 ACT，支持 ACT 协议的消息编解码、会话管理、服务调用、事件推送，实现阿里生态智能体无缝接入；

c) 支持异构智能体无障碍接入，不限制技术栈、开发框架、部署形态，接入无需大规模改造，实现即插即用；

d) 具备协议自动适配与转换能力，可自动识别接入协议并完成格式转换、语义对齐、消息路由，保障不同协议智能体间稳定交互。

6.1.3 注册后自动功能测试、能力核验、版本管理，具体要求如下：

a) 智能体完成身份注册并通过资质审核后，自动触发全链路自动化测试，覆盖服务可用性、意图响应准确率、接口稳定性、支付交互兼容性、合规校验完整性、异常容错能力等核心项；

b) 自动开展能力核验，对照智能体声明的服务能力，逐项验证实际执行效果，确保声明与实际一致，不合格不予接入；

c) 建立全生命周期版本管理机制，支持版本编号、灰度发布、在线升级、版本回滚、变更审计、能力基线对比，保障智能体服务持续迭代、风险可控；

d) 自动生成注册-测试-核验报告，留存测试用例、结果、异常日志，纳入智能体 DNS 审计体系，全程可追溯、可复核。

6.2 大语言模型能力

6.2.1 意图解析

6.2.1.1 支持口语化、自然语言、多轮碎片化、简略化、场景化输入，兼容文本、语音输入方式。
6.2.1.2 可自动识别模糊表达、省略成分、隐含需求，准确提取消费品类、价格区间、时间、地点、服务方式等关键结构化参数。
6.2.1.3 应支持多模态意图融合理解，能结合上下文与场景信息提升理解精度。

6.2.2 任务规划

6.2.2.1 应具备复杂任务自动拆解能力，将用户消费需求拆分为有序、可执行的原子任务序列。
6.2.2.2 应对输出标准、可机器解析的轻量级数据交换格式执行计划，包含任务编号、类型、依赖关系、执行主体、调用工具、输入输出、异常分支。
6.2.2.3 应支持并行+混合任务流，能识别并合理调度并行子任务，提升执行效率。

6.2.3 多轮对话

6.2.3.1 具备长会话记忆能力，支持多轮交互中上下文保持、信息复用、意图延续。
6.2.3.2 支持用户追问细节、补充条件、修改需求、变更订单、取消交易、撤销指令。

6.2.4 部署

应部署支持私有化+API Key双模式，实现模型与数据不出域和快速接入、按需调用、弹性扩缩容。私有化部署支持模型微调、领域知识注入、算力弹性扩容、安全隔离。云端调用支持权限控制、调用限流、计费统计、访问审计、异常告警。

6.2.5 大模型安全管控要求

针对数字人民币消费支付金融场景，应建立大模型特有风险安全管控机制，相关安全管控应符合GB/T 45654—2025规定，具体要求如下：

a) 幻觉控制：应采取知识库比对、事实校验、业务规则约束等手段，抑制模型幻觉；涉及交易指令、金额、资质、资金相关关键输出，不应直接采信模型生成结论，关键业务参数应做校验，避免虚假事实引发错误交易；
b) 提示词攻击防御：应具备识别并抵御指令注入、角色诱导、上下文污染等提示词攻击能力，防范通过恶意提示词绕过业务、安全约束，越权发起支付、查询等风险行为；
c) 输出内容安全审核：应对模型输入、输出开展安全审核，拦截违法违规、敏感泄露类内容；涉及交易执行类输出应当经过业务规则校验后方可交付上层智能体执行；
d) 模型偏见与公平性：开展模型偏见风险评估，防范地域、商户类型、用户群体带来算法歧视；不得因非业务必要因素区别对待不同消费者、不同中小商户，保障消费业务公平开展。

6.3 商户智能体

6.3.1 零代码创建

商户无需编程及技术背景，填写基础信息即可一键生成专属智能体，系统自动完成身份注册、能力配置、权限分配、网络接入及初始化配置，支持批量创建，快速接入智能体互联网。

6.3.2 商户管理

支持图文混合上传与结构化信息录入，提供批量操作、库存更新等功能，商品变更实时同步，保障信息准确有效。

6.3.3 订单履约

接收订单后自动推送至对应系统并生成标准订单，支持履约环节自动触发，订单状态双向实时通知，履约结果闭环可追溯。

6.3.4 数据看板

提供可视化运营数据看板，自动统计核心经营指标与用户画像信息，支持多维度数据查询与分析，辅助商户经营决策。

6.4 数字人民币智能支付

6.4.1 支付流程

支付全链路严格遵循标准化流程，依次完成用户消费意图确认、商户经营资质与数字人民币备案核验、数字人民币支付指令执行、多方智能合约自动分账、全交易链路区块链存证，确保每笔交易合规有序、流程闭环。

6.4.2 智能合约

内置可编程数字人民币智能合约，支持交易后多方自动分账、预付费资金专户监管、履约异常自动退款、预约服务到期自动履约，实现资金管理自动化、风险可控化。

6.4.3 双离线

支持数字人民币双离线支付能力，可在无网络环境下完成交易发起、身份核验与凭证生成，网络恢复后自动同步交易数据并完成清算对账，保障弱网场景支付连续性。

6.4.4 清算

实现数字人民币交易实时清算，资金划转即时到账，交易流水、分账明细全程公开透明，所有交易数据可查询、可审计、可追溯，满足金融合规监管要求。

6.5 MCP 接入要求

6.5.1 应支持流式传输模式、标准输入输出模式、开放 API 模式三种标准接入模式，覆盖实时交互、轻量工具调用、标准化接口对接等不同场景，适配各类外部系统与服务接入需求，统一接入框架、统一交互规范。

6.5.2 工具调用稳定可靠，具备高可用性，支持正常业务场景下稳定调用，响应及时，可保障业务流畅运行，具备异常容错与自动恢复能力。

6.5.3 应建立全链路调用日志记录机制，完整留存调用过程信息，敏感数据自动脱敏处理，日志信息加密存储、不可篡改，满足合规追溯与安全审计要求。

7 数字消费场景要求

7.1 线下商圈消费

7.1.1 用户通过轻量化 H5 入口提交消费需求，经大模型意图解析、智能体精准匹配、订单生成、数字人民币支付、商户履约、全链路区块链存证，形成闭环消费流程。

7.1.2 应构建“货找人”智能消费模式，支持无感支付、自动核销、商圈统一清算，简化消费环节，提升商圈消费效率与体验。商圈运营方、入驻商户、消费者、持牌机构应做好业务协同，明确订单流转、资金清算、售后处置各方业务分工。

7.1.3 支持智能穿戴等复杂物联网边缘节点设备接入场景。设备与数字钱包开展深度业务协同，可在边缘设备完成用户意图触发、交互指令采集；设备与后台系统之间应采用安全传输协议，对设备侧上行意图、支付交互信令进行加密、完整性校验、设备身份鉴权；防范指令篡改、设备仿冒、中间人劫持风险。物联网设备接入应遵循设备数据管理相关标准，设备采集个人数据遵循最小必要原则。

7.1.4 线下商圈场景开展智能体消费服务，应设置清晰的用户告知提示，向消费者说明智能体服务范围、授权事项、扣费规则、撤销方式；针对大额、高风险消费业务，落实人工审批提醒机制。

7.2 线上商城消费

7.2.1 支持全品类商品智能推荐、多商户比价、预约下单、数字人民币合约支付、自动发货及售后协同，覆盖线上消费全流程，满足多样化线上购物需求。
7.2.2 开展多商户比价服务时，应保证比价信息客观真实，不得设置算法偏向，不得刻意屏蔽中小商户商品；商品价格、库存、履约时效信息应与商户实际经营数据保持同步。
7.2.3 应支持智能售后协同，针对退货、换货、部分退款业务，由消费智能体、商户智能体、智付智能体协同完成业务受理、核验、资金处理；售后处理进度应及时向用户同步告知。
7.2.4 涉及预售类线上消费业务，应依托数字人民币智能合约做好资金管控，明确履约触发条件、退款规则，保护消费者资金权益。

7.3 生活缴费

7.3.1 支持水电燃气、通信、物业等账单自动生成、到期提醒、批量代缴、逾期风险拦截，依托 HEARTBEAT 主动触发机制实现周期性自动缴费，保障生活服务便捷高效。
7.3.2 开启周期性自动缴费前，应取得用户明确业务授权，明确缴费项目、扣款限额、执行周期、授权有效期；向用户提供便捷的授权查询、暂停、撤销操作入口。
7.3.3 每次自动扣费执行前宜向用户发送业务提醒；发生余额不足、缴费失败等情形，应及时告知用户并说明失败原因，避免产生持续性异常扣费。
7.3.4 缴费业务应留存完整账单核对记录，支持用户查询历史缴费明细。

7.4 文旅/景区消费

7.4.1 支持预约购票、入园核销、退票改签、分时履约、先履约后扣款，适配文旅场景灵活消费需求，优化文旅消费服务流程。
7.4.2 预约类业务应明确预约生效条件、改期、退票规则，规则对用户清晰可见；因景区限流、活动调整等客观因素无法履约时，智能体应自动触发退款或协助用户完成改期。
7.4.3 实施先履约后扣款模式时，应设置单次、周期扣款上限；扣款触发前核对用户业务授权有效性，避免无授权扣款。
7.4.4 针对团体购票、批量预约等高风险业务，应纳入 L3 人工审批管理。

7.5 预付费消费

7.5.1 启用数字人民币智能合约，应执行一课一结、一笔一清、资金专户监管、异常冻结、退款保障，防范预付费资金风险，保障消费者资金安全与权益。
7.5.2 预付费服务开通时，应向消费者清晰展示服务项目、服务有效期、资金使用规则、退款条件、合约冻结触发情形。
7.5.3 出现商户经营异常、服务终止等情形，智能合约应按约定对专户内剩余预付费资金执行冻结、退款处置；业务处置结果及时告知消费者。
7.5.4 预付费场景下商户智能体启用，应完成持牌机构商户尽职调查审核，方可开展预付费相关业务

8 安全与合规

8.1 数据安全

8.1.1 数据处理活动应遵循《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》相关规定，并符合 GB/T 35273 的相关要求。实施数据分级分类管控，遵循最小必要采集原则；对敏感个人信息应采取脱敏、加密等安全防护措施。核心数据宜在受控安全域内开展存储与处理，确需对外提供数据的，应符合法律法规及监管制度要求。不同类型数据最低留存期限应符合法律、行政法规规定，具体要求如下：

a) 交易流水、清算记录、审计日志等交易类数据：自交易结束之日起至少保存 10 年；如涉及未完结反洗钱调查，应延续保存至调查终结；
b) 用户身份核验资料：自业务关系结束或者一次性金融服务完成之日起至少保存 10 年；
c) 商户经营业务数据：按照商户授权约定的期限留存；授权到期后，在无其他法定留存义务情形下应自动删除或者做匿名化处理。

8.1.2 核心数据宜在受控安全域内开展存储与处理，应对外提供数据的，应符合法律法规及监管制度要求。交易、操作日志留存期限应满足反洗钱等监管时限要求，保障数据安全合规。

8.2 交易安全

应构建全方位交易安全防护体系，系统安全防护应符合 GB/T 22239—2019安全要求，具备防重放、防篡改、防冒用能力，实时拦截异常交易行为；所有交易数据进行区块链存证的，还应满足GB/T 42571—2023相关规范要求，实现交易数据不可篡改、全程可追溯，保障交易安全可靠。

8.3 合规要求

遵守金融监管规定，落实反洗钱全量报送要求，提升反欺诈识别能力；实现商户、用户资质全覆盖核验，快速响应监管新规并同步更新，确保全流程合规运营。

8.4 交易风险下各方权责划分

8.4.1 用户授权形式与授权范围限定

8.4.1.1 开展 AI 智付交易前，应取得用户明确、具体、可查验的有效授权。授权可采用电子协议、书面确认、经身份核验的语音确认等形式；授权文件应当清晰载明可执行交易类型、交易限额、扣款账户、有效期限、业务场景，禁止笼统、概括式的一揽子无限授权。

8.4.1.2 授权的成立以用户完成身份核验、主动确认授权内容为要件；发生授权变更、到期、用户主动撤回、用户账户注销情形时，授权即时终止，智能体不得再发起任何支付类交易。系统应当完整留存授权全生命周期记录，包含授权设立、变更、终止的时间与操作凭证。

8.4.2 智能体支付指令的行为归属

智能体不具备独立民事主体资格，仅作为用户意志的技术执行载体。在用户有效授权范围内，智能体所发起的数字人民币支付指令，视为用户委托执行的交易指令；超出有效授权范围的，不能归属于用户交易意思表示。全链路审计日志、授权记录、智能体行为记录是判断指令是否处于授权边界内的核心凭证。

8.4.3 越权交易、误操作的资金损失与责任分担

越权交易、误操作的资金损失与责任分担内容如下：

a) 在用户有效授权范围内，因用户自身指令、输入歧义导致交易结果偏差，由用户承担相应后果；
b) 因智能体开发方、技术服务商的代码缺陷、算法缺陷、安全漏洞、权限管控失效，引发越权交易、错误交易，造成用户资金损失的，智能体开发方 / 技术服务商应当依法承担相应赔偿责任；涉及持牌机构业务环节过错的，由对应持牌机构承担相应责任；
c) 技术服务商、智能体开发方应当建立先行赔付工作机制，对于经核实属于己方责任造成的用户资金损失，按照约定及时开展先行赔付，之后可向过错责任方追偿；
d) 多方混合过错造成损失的，依据各方过错程度分担损失。

8.4.4 用户撤销权与交易回滚机制

8.4.4.1 用户享有随时全部或部分撤销智能体交易授权的权利；系统收到撤销指令后应在规定时限内生效，立即阻止智能体发起新的支付交易。

8.4.4.2 对于尚未完成清算的交易，用户提出撤销申请时，系统应具备交易中止、回滚能力；对于已经完成清算的交易，通过退款、纠纷处置流程处理。

8.4.4.3 应向用户提供便捷的授权查询、授权撤回、交易异议申诉操作入口，完整留存撤销、异议申诉操作日志。

9 运维与应急

9.1 日常运维

建立常态化运维管理机制，实行7×24 h全链路实时监控，保障系统稳定运行。

采用灰度发布策略，降低版本迭代风险；定期开展安全扫描与漏洞检测，及时消除安全隐患。规范日志留存管理，确保可追溯、可审，实施全生命周期版本管理，支持迭代优化与回退。

9.2 应急处置

建立分级应急响应机制：

a) P0（核心中断）：核心业务不可用，15 min 内响应，快速处置恢复；
b) P1（功能异常）：部分功能故障，30 min 内响应，排查修复；
c) P2（性能下降）：系统性能劣化，2 h 内响应，优化恢复；
d) 灾备保障：采用多活部署、数据备份、快速切换机制，应对极端故障，确保业务连续性。

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）人民日报.

[5] 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764号，2023-12-09（2024-05-01施行）中国政府网.

[6] 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）.

[7] 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）中国政府网.