数据可信空间完整解决方案

一、项目概述与产品定位

1.1 合规依据补充

本次项目严格遵循国家及地方现行数据合规法规，除原有法律外，增补《政务数据共享交换平台建设指南》《信创服务器软硬件兼容适配规范》《区块链信息服务管理规定》，同时贴合本地政务内网等保三级建设细则，杜绝合规漏洞。

1.2 项目背景

当前政务跨部门、政企、行业联盟间数据流通存在三大痛点：一是数据资产台账分散，各部门数据孤岛严重，无统一目录管理；二是数据流转不可控，明文传输易泄露、越权访问无法拦截；三是数据操作无全链路溯源，出现数据篡改、外泄后无法定位责任主体。同时政务数据需满足《数据安全法》《个人信息保护法》、网络安全等级保护 2.0 三级合规要求，传统数据共享平台采用数据拷贝外放模式，无法实现数据“可用不可见、可控可溯源”，一旦发生数据泄露，监管追责风险极高。

1.3 产品定位

数据可信空间系统是面向政务跨委办局、国资企业、产业链联盟的跨主体数据协同底座，基于隐私计算、联盟区块链存证、细粒度动态权限管控三大自研可信技术，独立部署于政务内网安全隔离域，全程不触碰、不落地原始核心数据明文，支持跨主体离线点对点协同、内网在线密文流转，适配政务零外网穿透的安全管控要求。

1.4 建设基本原则

新增轻量化建设原则，贴合政务方案标准：1.安全内生原则：所有可信能力内嵌于流转链路，不新增数据暴露节点；2.国产化全栈适配原则：软硬件 100%适配鲲鹏、海光国产芯片，无境外开源高危组件；3.最小改动原则：对接现有政务存量系统，不重构原有业务数据库；4.权责分离原则：运维、审计、审批账号三权分立，杜绝单人全权限操作。

1.5 五大核心目标

资产底座：全域采集结构化、非结构化政务数据，构建分级分类统一数据资产目录，完成数据标签、敏感等级、归属部门标注，资产台账更新时效≤1 小时，支持资产变动自动告警

流转底座：搭建基于隐私求交、安全聚合的可信交换链路，数据流转全程密文传输，源头数据不出本地库，原始数据零跨节点迁移

审计底座：基于联盟区块链实现全操作日志存证，日志哈希值永久不可篡改，支持司法公证处直接调取证据链，满足司法举证要求

风控底座：内置敏感数据识别、越权访问、批量导出异常三大风控模型，实现 7*24 小时自动告警、实时链路阻断，告警响应时延≤3 秒

协同底座：支持不少于 20 个异构政务节点跨区域互联互通，兼容政务现有大数据平台、统一身份认证平台、电子签章平台三方接口

二、全量用户角色明细与权责边界

按照数据所有权、使用权、管理权三方拆分，共 6 类核心角色，严格执行账号独立、权限互斥、操作留痕，杜绝权责交叉，补充每类角色账号使用约束：

数据提供方管理员：所属部门数据资产录入、敏感等级标注、流转授权审批、本节点风险核查；约束：无权跨节点修改外部数据，审批操作不可撤回，自动上链存证

数据使用方业务人员：资产目录查询、数据集脱敏预览、数据交换申请、个人操作审计日志自查；约束：无法查看原始明文数据，仅可查看脱敏后字段内容

跨节点审批专员：跨主体数据流转二级合规审查、申请驳回/通过、流转时效管控；约束：仅负责合规审核，不干预数据业务使用场景

平台运维管理员：节点接入、用户角色配置、服务器监控、系统补丁更新；硬性约束：无任何原始数据、脱敏数据查看权限，操作全程被安全审计员监控

安全审计员：独立物理隔离账号，仅可查看全链路审计日志、风险告警记录；约束：不可修改、删除任何业务与日志数据，账号密码双人保管

监管督察员：上级监管部门专属账号，全域节点数据流通统计、违规事件溯源、合规报表导出；约束：仅拥有只读权限，无法下发审批指令

三、产品功能架构与页面结构

3.1 分层功能架构

自上而下分为四层，修正原有扁平化架构缺陷，层间采用 API 网关隔离，防止横向越权：前端交互层、业务应用层、可信能力中台、底层基础设施层

前端交互层：包含顶部导航、左侧固定菜单、卡片化主内容区，统一政务蓝白政企 UI 规范，适配国产化浏览器无障碍访问

业务应用层：系统总览、数据资产目录、数据集详情、可信流转链路、交换申请、权限与授权、可信审计、风险告警、节点管理、用户与角色（10 大核心模块）

可信能力中台：区块链存证引擎、隐私计算引擎、细粒度鉴权引擎、敏感数据识别引擎、日志存证引擎；中台独立部署，不与业务层共用服务器资源

基础设施层：服务器集群、政务内网交换机、工业防火墙、数据备份存储、单向安全网闸，所有设备纳入政务内网资产台账

3.2 全局页面结构

页面采用政务系统主流三分屏布局，全局样式统一，适配 1920*1080、1366*768 两类政务办公屏幕分辨率：

顶部导航（固定置顶，不随页面滚动）：政务 Logo、全局模糊搜索、站内消息通知、个人用户中心、全局系统设置 5 项，消息未读角标红色高亮，告警消息优先级高于普通通知

左侧菜单栏（固定收起/展开切换）：10 项核心模块，根据用户角色动态隐藏无权限菜单，菜单访问路径记录至审计日志

主内容区：统一四分区排布，顶部指标卡片、中部可视化图表、底部数据列表、列表内嵌单行操作按钮，全部列表支持多条件组合筛选、批量导出、分页、排序，导出文件自动加水印溯源

四、核心标准化业务流程

4.1 跨部门数据交换申请全流程

数据使用方查询资产目录→查看数据集敏感等级、使用限制→提交交换申请（填写使用用途、时效、数据范围、对外使用场景）→系统自动前置敏感合规初审→数据提供方业务审批→跨节点安全专员复核→动态授权开通访问权限→密文可信流转→全

链路日志区块链存证审计→权限到期自动回收

补充分支逻辑：初审识别到高敏感数据（人脸、户籍、征信），直接驳回申请，无需人工审批，同步推送风险通知至双方管理员及本级安全审计员，留存驳回记录永久归档

4.2 数据可信流转底层流程

本地业务数据库原始数据接入→数据来源确权（绑定部门节点、操作人员身份、设备 IP）→本地脱敏+同态加密双重处理→跨节点网闸权限校验→授权后密文点对点流转→多方安全联合计算（原始数据不出域、不迁移）→计算结果脱敏输出→所有流转节点、操作人员、时间戳、IP 地址、设备编号上链存证

4.3 风险闭环处置流程

系统 AI 引擎识别异常（批量下载、异地 IP 访问、超时效访问、高频预览）→分级告警（一般/较大/重大）→安全审计员 1 小时内人工核实→一般风险：合规确认后关闭告警，留存台账；较大风险：临时冻结用户权限、短信告知用户；重大风险：自动阻断跨节点数据访问、切断链路、上报上级监管部门，同步生成标准化风险处置报告，报告同步上链

五、十大核心页面详细需求

统一交互规范：全部页面遵循卡片化布局、风险三色标识（绿色正常、黄色预警、红色高危）、审批链路可视化、权限配置树形结构化，符合政务 PRD 交互原则，所有页面操作时延统一纳入性能考核

5.1 系统总览

页面组成：全域资产指标卡片（资产总数、敏感资产占比）、节点在线拓扑图、近期流转趋势折线图、未办结申请统计、高危风险告警快捷入口。操作链路：拓扑图点击异常节点→跳转链路详情→查看分钟级时间线事件，支持拓扑图一键导出 PDF 用于周报上报

5.2 数据资产目录

页面组成：资产分类树形筛选、敏感等级标签筛选、资产列表（名称、归属部门、更新时间、敏感等级、流转状态）、资产批量标签编辑。操作链路：列表点击资

产→数据集详情页→发起临时/长期交换申请，临时权限最长有效期 90 天，长期权限需监管部门备案

5.3 数据集详情

页面组成：基础属性面板、数据表字段结构预览、已授权用户清单、历史流转记录、字段脱敏规则。操作链路：查看脱敏字段明细→针对指定字段申请定向数据开放，支持单字段、多字段精细化授权，不支持全表无差别开放

5.4 可信流转链路

页面组成：跨节点链路拓扑、链路时延、数据传输量、链路异常记录、操作时间线。操作链路：异常链路详情→调取区块链存证证据原文，支持证据原文对接公证处核验接口

5.5 交换申请

页面组成：待我审批、我发起、已办结、已驳回四个标签页，申请单包含用途、时效、数据范围、合规初审意见。操作链路：查看申请附件→填写审批意见→通过/驳回并填写驳回原因，所有审批意见不可修改，永久留痕

5.6 权限与授权

页面组成：用户权限清单、动态授权策略模板、字段级白名单、时效管控配置。操作链路：新增策略→配置 IP、时段、数据字段三维访问范围，支持权限到期自动提醒、提前回收

5.7 可信审计

页面组成：用户操作审计、数据流转审计、权限变更审计、区块链证据导出。操作链路：操作详情→核验上链哈希值→出具司法合规审计报告，报告自带区块链核验二维码

5.8 风险告警

页面组成：告警分级列表、异常行为溯源、处置进度看板。操作链路：告警核实→一键关闭/升级阻断，自动同步处置记录至审计台账，禁止人工删除告警记录

5.9 节点管理

页面组成：内外网节点清单、节点带宽、版本、在线状态、拓扑关联关系。操作链路：离线节点排查→查看节点间端口连通拓扑，支持节点离线自动告警

5.10 用户与角色

页面组成：用户账号列表、角色树形权限模板、身份关联政务统一认证。操作链路：新增用户→绑定预设角色→微调个性化字段权限，用户账号强制开启双因素认证

六、非功能需求

性能需求：单节点并发访问≥300 用户，页面响应时延≤1.5s，跨节点数据流转时延≤5s，区块链上链时延≤2s，系统 7*24 小时可用，年度可用性≥99.95%，大促批量流转场景无链路拥堵

兼容性需求：适配政务内网浏览器（360 安全浏览器、麒麟浏览器），兼容国产化操作系统银河麒麟 V10、达梦数据库、鲲鹏 ARM/海光 x86 双架构服务器，无需额外适配补丁

安全需求：满足等保三级、数据分类分级合规，账号双因素登录，传输链路 TLS1.3 加密，原始数据不落地应用服务器，服务器内网零外网 IP 映射

扩展性需求：支持横向新增节点接入，无需重构底层代码，预留政务大数据平台、统一身份认证、电子签章三方接口，接口遵循政务开放 API 规范

七、服务器分层部署方案

结合政务内网物理隔离、国产化替代、等保三级要求，采用内网三区两域云边集群部署，分为边缘可信节点、应用业务域、数据存储域、区块链存证域，全部部署于政务专有内网，物理隔离互联网，禁止外网穿透、禁止内网主机双网卡混用。

7.1 整体部署拓扑

边缘节点（各委办局本地机房）→政务内网核心交换机→防火墙单向网闸→中心机房应用集群+存储集群+区块链集群；网闸配置单向只读策略，仅允许边缘向中心上传数据，禁止反向回传

7.2 硬件服务器明细

服务器类型	数量	硬件配置	部署用途
边缘可信服务器（委办局）	每节点 1 主 1 备	鲲鹏 920 32 核、64G 内存、2TB SSD、国产加密卡	本地数据脱敏、加密、断网离线流转，本地原始数据存储，不向中心机房同步原始数据
应用负载服务器（中心机房）	3 台集群	鲲鹏 920 48 核、128G 内存、4TB SSD	前端业务、权限管控、申请审批、页面接口服务，Nginx 负载均衡，故障自动切换
数据库服务器（主从分离）	2 主 2 从	鲲鹏 920 64 核、256G 内存、全闪存储阵列	主库：业务实时读写；从库：审计、报表查询，读写分离降负载，主库故障 1 分钟自动切换从库
区块链存证服务器	4 节点联盟集群	海光 5380、96G 内存、8TB 机械硬盘	操作日志、流转记录哈希存证，数据永久不可篡改，4 节点异地分片存储，单节点宕机不影响链服务
备份存储 NAS	1 套双控	裸容量 48TB，支持快照备份	审计日志、配置文件异地备份，满足 90 天溯源留存要求，备份数据半年一次离线冷备份

7.3 底层软件环境

操作系统：银河麒麟服务器 V10 SP3（ARM 版），关闭系统多余默认端口，禁用

无用系统服务

数据库：达梦 8 国产分布式数据库、InfluxDB 时序数据库（存储链路监控数据），数据库开启透明数据加密 TDE

中间件：东方通应用服务器、Redis 6.2、RabbitMQ 消息队列，中间件定期漏洞扫描，每月补丁更新

可信组件：国产同态加密套件、长安链联盟链底层，通过国家密码局商用密码认证

7.4 网络安全隔离部署

VLAN 网段隔离：划分业务网、存储网、区块链网三个独立网段，网段间通过工业防火墙隔离，禁止跨网段直接访问，仅开放最小必要端口

边界安全：委办局与中心机房之间部署单向安全网闸，仅允许密文日志、哈希数据单向上传，禁止原始数据回流

账号安全：服务器禁用 root 远程登录，启用密钥登录，每 90 天自动轮换密码，端口全量白名单管控，远程运维仅允许内网堡垒机接入

7.5 容灾与运维方案

断电容灾：中心机房配套 UPS 不间断电源，续航 3 小时，保障峰值业务平稳停机，断电后自动触发链路保护，终止所有数据流转

数据容灾：每日凌晨全量异地备份，每 4 小时增量快照备份，备份数据异地机房存储，数据恢复时长≤2 小时，恢复后自动核验数据哈希一致性

离线容灾：边缘节点断网后可独立运行 72 小时，内网恢复后自动同步所有离线操作日志，不丢失业务数据，同步完成链上补存

日常运维：系统内嵌运维监控大屏，同步监控服务器 CPU、内存、磁盘、端口异常，告警同步推送系统风险中心及运维人员内网短信终端

八、项目风险识别与应对措施

8.1 技术适配风险

风险：存量政务老旧系统接口协议不兼容，导致资产采集失败；应对：提前开展

3 天存量系统接口摸排，定制轻量适配网关，不改造原有老旧系统

8.2 内网部署风险

风险：政务内网无外网无法获取系统补丁，存在漏洞隐患；应对：建立内网离线补丁库，每月通过涉密 U 盘单向导入合规补丁，全程留痕审计

8.3 人员使用风险

风险：业务人员违规绕过系统私下传输数据；应对：对接内网终端管控系统，阻断内网文件跨部门拷贝，终端操作同步纳入可信审计

九、验收标准

9.1 功能验收

10 大模块功能 100%匹配 PRD 需求，数据交换审批链路完整，区块链证据可导出核验，风险告警处置闭环率 100%，用户角色权限零越权漏洞，第三方渗透测试无高危漏洞

9.2 性能验收

并发 300 用户稳定运行 72 小时无宕机，页面响应≤1.5s，跨节点流转时延≤5s，日志上链成功率 100%，极端并发场景 CPU 占用率不超过 80%

9.3 部署验收

完成国产化服务器集群部署，通过网络安全等级保护三级测评，内网物理隔离合规，接口对接现有政务统一认证平台成功，出具国产化软硬件兼容适配报告

十、项目实施组织、周期与运维保障

10.1 实施人员分工

项目组分为：需求对接组（2 人，对接各委办局数据口径）、部署实施组（3 人，服务器与网络部署）、安全测评组（2 人，等保合规整改）、售后运维组（1 人，常驻内网运维）

10.2 实施周期

需求细化 5 天：存量数据摸排、接口确认、权限口径定稿；软硬件部署 10 天：服务器上架、网络配置、国产化系统安装；功能开发联调 20 天：接口对接、功能自测、权限配置；等保合规整改 5 天：漏洞修复、安全策略加固；压力测试+验收 5 天：第三方压测、资料归档、现场验收

10.3 售后运维保障

提供 3 年 7*24 小时内网远程运维服务，内网故障 2 小时响应、4 小时现场处置；每季度开展一次系统安全巡检、日志复盘；每年免费完成一次系统版本轻量化迭代

十一、项目合规依据与综合价值

11.1 合规依据清单

《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》《网络安全等级保护 2.0》《商用密码应用安全性评估管理办法》《政务数据共享开放技术要求》

11.2 量化产品价值

安全价值：消除明文数据共享泄露风险，满足等保三级、商密测评双合规，规避单次最高 1000 万元数据违法处罚；业务价值：跨部门数据协同效率提升 70%，无需人工线下数据报送；监管价值：实现数据全链路司法溯源，满足上级数据督查常态化核查要求；信创价值：全栈国产化软硬件，完成政务信创替代考核指标。

本方案依托国产化服务器云边协同部署，实现政务多主体数据可用不可见、可控可计量、全程可溯源，解决数据孤岛、数据泄露、责任无法溯源三大痛点，完全符合国家数据安全及国产化信创要求，可直接用于政企招投标、内部立项、项目交付。

