ICS 35.020
CCS L 79

T/ZPP

团 体 标 准

T/ZPP 149—2025

跨域可信数据运维管理技术规范

Technical specification for cross-domain trusted data operation and maintenance management

2025－06－27 发布　　2025－06－30 实施

浙江省品牌建设促进会　　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　总体架构 1
5　数据治理要求 2
6　跨域数据传输技术 4
7　可信数据存储 6
8　运维监控与应急 7

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。

本文件由杭州觉起科技有限公司提出。

本文件由浙江省品牌建设促进会归口。

本文件起草单位：杭州觉起科技有限公司、宁波中铖信息科技有限公司、浙江六久科技有限公司、浙江净禾智慧科技有限公司、杭州半云科技有限公司、杭州智海合达科技有限公司、杭州赛普特信息科技有限公司、杭州纵横通信股份有限公司、浙江云茗科技有限公司、杭州创新易软件有限公司、浙江雨林电子科技有限公司、杭州协能科技股份有限公司、中科润禾(杭州)信息技术有限公司、杭州美帮网络科技有限公司、杭州智海合达科技有限公司、杭州宇泛智能科技股份有限公司、品茗科技股份有限公司、宁波市科技园区明天医网科技有限公司、杭州聚达物联科技有限公司、浙江中杭电子有限公司、信雅达科技股份有限公司、杭州荣融通信技术有限公司、浙江华安技术有限公司、杭州市钱塘医院、杭州信雅达泛泰科技有限公司、浙江达摩网络科技有限公司、杭州物必连科技有限公司、杭州长勺智能科技有限公司、杭州安佳通信工程有限公司、杭州远泰通信工程有限公司、杭州君辰电子科技有限公司、杭州长勺智能科技有限公司。

本文件主要起草人：王晶、汪家斌、余志飞、朱新荣、陈细平、陈思、朱明、冯益君、余世国、杨萱、钟圣佑、陈秋兰、吴文、汪晖、沈云波、吴红宇、吴懿红、俞琦莺、项方云、殷金旗、黄龙、叶茂允、蔡昌伟、江成飞、刘德志、蔡华满、胡顺扬、楼静斐、王启宏、祝骅、王吉国、马小飞、徐涛、杨卫、杨旭华、袁金慧、张金名、张文娟、张鑫、张延闹、郑星港、朱群锋、吴桂林、李莉、赵来福、雷学俊、徐洋、吴彩霞、吴桂林、杨诗萍。

跨域可信数据运维管理技术规范

1 范围

本文件规定了跨域可信数据运维管理的术语和定义、总体架构、数据治理要求、跨域数据传输技术、可信数据存储、运维监控与应急。

本文件适用于跨域可信数据运维管理。

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 38633 信息技术 大数据 系统运维和管理功能要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信数据 trusted data

指数据在采集、存储、传输和使用过程中，具有真实性、完整性、一致性、可用性和可验证性的特征，确保数据未经篡改，来源可靠，传输和处理过程中未被破坏或误用。

3.2

跨域 cross-domain

指数据或计算任务在两个及以上独立管理的数据域之间进行传输、共享或协同处理的操作。

4 总体架构

4.1 逻辑架构

4.1.1 数据资源层

4.1.1.1 数据资源层应实现跨域数据资源的统一标识、分类分级与元数据管理。

4.1.1.2 数据提供方宜建立数据资产目录，明确数据来源、敏感级别及使用约束条件。

4.1.1.3 各参与域应遵循统一的元数据标准，确保数据定义的一致性。

4.1.1.4 跨域数据共享时，原始数据宜保留在数据所属域内，仅通过标准化接口对外提供计算结果的交互能力。

4.1.2 可信计算层

4.1.2.1 可信计算层应提供身份认证、授权管理、隐私计算及过程溯源功能。

4.1.2.2 计算层宜采用去中心化架构，支持多参与方共同维护计算节点。

4.1.2.3 跨域计算任务发起时，应通过预定义安全策略验证参与方的合规性。

4.1.2.4 计算过程应实施全链路加密与行为审计，确保操作可追溯。

4.1.3 业务应用层

4.1.3.1 业务应用层应封装跨域数据服务的业务逻辑，提供标准化 API 接口。

4.1.3.2 应用层宜支持动态策略配置，自动适配不同敏感级别数据的访问规则。

4.1.3.3 跨域数据服务的结果输出应包含完整性校验信息，防止篡改。

4.1.4 跨域协作机制

4.1.4.1 跨域协作机制应通过共识算法保障操作一致性，建立多方信任锚点。
4.1.4.2 关键操作记录应同步至各参与方的审计节点，支持异议仲裁流程。
4.1.4.3 数据使用方提出计算请求时，应通过智能合约明确权责边界。

4.2 技术体系

4.2.1 身份认证与授权管理

4.2.1.1 参与方应具备唯一可验证的数字身份标识，宜采用公钥基础设施实现认证。
4.2.1.2 数据访问授权应遵循最小化原则，动态调整权限范围。
4.2.1.3 授权策略宜采用声明式描述语言，支持自动化策略解析与执行。

4.2.2 数据安全传输

4.2.2.1 跨域数据传输应建立端到端加密通道，确保机密性与完整性。
4.2.2.2 传输协议宜支持前向安全特性，防止历史数据因密钥泄露被解密。
4.2.2.3 高敏感数据可采用分片传输机制，单一分片不包含完整信息。

4.2.3 隐私增强计算

4.2.3.1 涉及多方数据融合的计算场景，应优先采用隐私计算技术。
4.2.3.2 宜根据需求选择联邦学习、安全多方计算或可信执行环境技术路线。
4.2.3.3 计算过程中应定期验证参与方的计算逻辑合规性。

4.2.4 审计溯源技术

4.2.4.1 跨域数据操作全流程应记录包含操作主体、时间戳等要素的审计日志。
4.2.4.2 审计系统宜采用分布式账本技术，通过哈希链关联多域日志记录。
4.2.4.3 发生争议时，可通过跨域审计日志的联合分析还原操作真相。

4.2.5 弹性安全防护

4.2.5.1 技术体系应具备动态风险感知与自适应防护能力。
4.2.5.2 宜构建跨域威胁情报共享机制，实时同步攻击特征库与防御策略。
4.2.5.3 检测到异常行为时，可自动触发熔断机制并启动人工复核流程。

4.3 实施原则

总体架构的实施应遵循以下原则：
——合规优先原则：技术选型与流程设计应符合数据安全法、个人信息保护法等法律法规要求；
——最小化暴露原则：数据传输与计算过程中应最大限度减少原始数据跨域流动；
——防御纵深原则：在不同层级部署差异化的安全控制措施，形成多层防护体系；
——开放兼容原则：核心组件宜采用标准化协议，支持与主流技术生态互通；
——持续演进原则：建立技术体系的版本化管理机制，定期评估新兴技术的适配性并迭代升级。

5 数据治理要求

5.1 元数据管理

5.1.1 元数据要求

5.1.1.1 元数据应包含数据的基本属性、业务属性及管理属性，基本属性宜涵盖数据名称、标识符、格式、存储位置等。
5.1.1.2 业务属性应明确数据的业务含义、关联关系及使用场景，管理属性应包含数据责任人、更新频率及访问权限等信息。

5.1.2 元数据标准化

5.1.2.1 各参与域应遵循统一的元数据标准，确保跨域数据描述的一致性。

5.1.2.2　元数据模型宜采用通用语义框架，支持机器可读和自动化解析。

5.1.3　元数据共享

5.1.3.1　跨域数据共享时，宜通过元数据目录对外发布数据资源的摘要信息。
5.1.3.2　元数据共享过程应进行完整性校验，防止篡改或伪造。

5.2　数据分类分级

5.2.1　分类框架

5.2.1.1　数据分类应基于业务领域、数据类型及使用目的划分，如公共数据、业务数据、隐私数据等。
5.2.1.2　分类框架宜支持动态扩展，以适应新增数据类型的管理需求。

5.2.2　分级要求

5.2.2.1　数据分级应依据敏感程度、影响范围等因素划分为多个级别，并定义各级别的防护要求。
5.2.2.2　分级标准应兼容国家及行业相关规范，避免跨域场景下的标准冲突。

5.2.3　跨域分级映射

5.2.3.1　参与域之间的数据分级差异应建立映射规则，确保跨域数据共享时级别判定的一致性。
5.2.3.2　参与域宜设立分级仲裁机制，处理分级标准不一致引发的争议。

5.3　数据质量管理

5.3.1　质量指标

5.3.1.1　应定义数据质量的核心指标，包括准确性、完整性、一致性、时效性等。
5.3.1.2　跨域数据质量评估宜采用多方协同验证机制，避免单方评估的主观偏差。

5.3.2　质量监控

5.3.2.1　应建立数据质量异常检测规则，如空值率阈值、格式合规性检查等。
5.3.2.2　检测到质量问题时，宜自动触发告警并生成修复工单。

5.3.3　质量修复

5.3.3.1　数据质量问题修复过程中应记录操作日志，确保修复过程可追溯。
5.3.3.2　修复后的数据宜重新进行跨域一致性校验，确认符合质量要求。

5.4　数据生命周期管理

5.4.1　创建与采集

5.4.1.1　数据创建时应自动关联元数据，并依据分类分级规则打标。
5.4.1.2　跨域数据采集宜采用轻量化传输协议，减少冗余数据流动。

5.4.2　存储与使用

5.4.2.1　存储系统应支持数据分域隔离，不同级别的数据宜采用差异化的加密策略。
5.4.2.2　数据使用过程应实施动态权限控制，超出授权范围的访问请求应自动拦截。

5.4.3　归档与销毁

5.4.3.1　归档数据应保留必要的元数据索引，支持后续审计与检索。
5.4.3.2　数据销毁应通过覆写或物理销毁等方式确保不可恢复，并记录销毁凭证。

5.5　数据合规审计

5.5.1　合规要求

5.5.1.1　数据治理活动应符合《数据安全法》《个人信息保护法》等法律法规要求。
5.5.1.2　涉及跨境数据流动时，宜额外遵循目标地区的合规性要求。

5.5.2 审计机制

5.5.2.1 应建立覆盖数据全生命周期的审计日志，记录关键操作事件。
5.5.2.2 审计日志宜采用防篡改存储技术，确保日志的真实性与完整性。

5.5.3 违规处置

5.5.3.1 发现数据违规行为时，应暂停相关数据服务并启动调查流程。
5.5.3.2 宜通过智能合约自动执行违规处罚条款，如权限回收或经济惩罚。

5.6 数据共享与协作机制

5.6.1 共享协议

5.6.1.1 跨域数据共享应签订多方协议，明确数据用途、使用期限及责任划分。
5.6.1.2 协议内容宜通过区块链存证，提供不可抵赖的法律效力。

5.6.2 协作流程

5.6.2.1 数据共享请求应通过统一接口提交，并经过多方协同审批。
5.6.2.2 协作过程中产生的衍生数据应明确权属归属规则。

5.6.3 争议解决

5.6.3.1 应设立跨域争议仲裁委员会，处理数据权属、质量等问题引发的纠纷。
5.6.3.2 仲裁结果宜通过技术手段强制执行，如冻结违规方数据访问权限。

6 跨域数据传输技术

6.1 传输协议

6.1.1 协议选型

6.1.1.1 跨域数据传输应优先采用具备加密和完整性校验能力的标准化协议。
6.1.1.2 宜选择支持前向安全特性的协议，防止历史会话密钥泄露导致数据解密风险。
6.1.1.3 协议应支持会话恢复机制，在网络中断后能快速重建连接并续传数据。

6.1.2 协议参数配置

6.1.2.1 加密算法应遵循国家密码管理部门核准的商用密码标准。
6.1.2.2 密钥交换参数宜定期更新，密钥有效期不应超过预设的安全周期。
6.1.2.3 协议超时时间应根据网络延迟特性动态调整，避免因超时导致传输失败。

6.2 安全通道建立

6.2.1 身份认证

6.2.1.1 通道建立前应对通信双方进行双向身份认证，确保参与方身份合法可信。
6.2.1.2 宜采用基于数字证书的认证机制，证书颁发机构应具备跨域互认资质。

6.2.2 密钥协商

6.2.2.1 密钥协商过程应使用抗量子计算攻击的算法，提升长期安全性。
6.2.2.2 临时会话密钥宜通过安全多方计算生成，避免密钥材料集中存储风险。

6.2.3 通道维护

6.2.3.1 应定期检测通道健康状态，异常时自动触发重协商或切换备用通道。
6.2.3.2 通道关闭后应彻底清除会话密钥及相关临时数据，防止残留信息泄露。

6.3 数据封装与解析

6.3.1 数据包结构

6.3.1.1 传输数据包应包含包头、载荷及签名三部分，包头宜包含版本号、数据类型标识等元信息。
6.3.1.2 签名部分应使用发送方私钥对数据包进行数字签名，确保来源真实性与完整性。

6.3.2 元数据关联

6.3.2.1 传输数据应与元数据绑定，接收方可依据元数据验证数据合规性。
6.3.2.2 敏感数据宜关联脱敏策略标识，指导接收方按规则处理数据内容。

6.3.3 编解码策略

6.3.3.1 数据编码宜采用紧凑二进制格式，减少传输带宽消耗。
6.3.3.2 编解码库应具备防御缓冲区溢出等安全漏洞的能力。

6.4 传输完整性保障

6.4.1 校验机制

6.4.1.1 传输数据应附加哈希校验值，接收方应验证校验值的一致性。
6.4.1.2 宜采用增量哈希算法，支持大文件分块传输时的逐块校验。

6.4.2 错误处理

6.4.2.1 校验失败时，接收方应丢弃异常数据块并请求重传。
6.4.2.2 连续传输失败超过阈值后，宜暂停传输并启动人工介入流程。

6.4.3 端到端验证

6.4.3.1 数据接收方应通过业务逻辑验证数据有效性，如格式合规性、业务规则匹配等。
6.4.3.2 验证结果应反馈至发送方，作为传输质量评估的依据。

6.5 传输性能优化

6.5.1 压缩技术

6.5.1.1 高冗余数据宜采用无损压缩算法减少传输数据量。
6.5.1.2 压缩算法应避免引入额外安全风险，如 ZipSlip 路径穿越漏洞。

6.5.2 分片传输

6.5.2.1 大规模数据宜分片传输，单个分片大小应根据网络 MTU 动态调整。
6.5.2.2 分片传输应保证顺序性，接收方应验证分片序号连续性。

6.5.3 多路径传输

6.5.3.1 关键数据可启用多路径并行传输，提升传输可靠性。
6.5.3.2 多路径传输时应避免同一数据分片在多个通道重复发送。

6.6 传输过程审计

6.6.1 日志记录

6.6.1.1 应记录传输任务的起止时间、数据量、参与方身份等核心信息。
6.6.1.2 审计日志宜包含传输路径拓扑信息，支持事后链路分析。

6.6.2 追溯机制

6.6.2.1 传输数据包应嵌入可追溯标识，支持跨域数据流转路径还原。
6.6.2.2 追溯标识宜与区块链存证系统关联，提供不可篡改的溯源证据。

6.6.3 异常检测

6.6.3.1 应实时监控传输速率、丢包率等指标，超出合理范围时触发告警。

6.6.3.2　检测到疑似恶意攻击行为时，可立即终止传输并隔离可疑节点。

7　可信数据存储

7.1　存储架构

7.1.1　分布式存储架构

7.1.1.1　跨域数据存储应基于分布式架构设计，支持多节点协同存储与负载均衡。
7.1.1.2　存储节点宜部署于不同物理或逻辑域内，避免单点故障导致数据不可用。
7.1.1.3　存储系统应提供跨域数据路由功能，确保数据访问请求定向至最近节点。

7.1.2　多副本策略

7.1.2.1　关键数据应存储至少三个副本，副本分布宜满足地理隔离要求。
7.1.2.2　副本一致性协议应支持最终一致性或强一致性模式，并依据业务需求配置。

7.1.3　跨域存储协作

7.1.3.1　跨域数据存储应通过智能合约约定存储责任方及服务质量指标。
7.1.3.2　数据存储状态变更时，宜通过事件通知机制同步至相关参与方。

7.2　冗余与备份

7.2.1　冗余策略

7.2.1.1　冗余数据应通过纠删码或镜像技术实现，平衡存储效率与可靠性。
7.2.1.2　冗余策略参数宜根据数据敏感级别动态调整，高敏感数据可增加冗余度。

7.2.2　备份管理

7.2.2.1　应制定定期备份计划，备份频率宜与数据更新频率匹配。
7.2.2.2　备份数据应存储于独立的安全域，并与生产环境物理隔离。

7.2.3　备份恢复

7.2.3.1　应建立备份数据完整性验证机制，确保恢复时数据可用。
7.2.3.2　恢复操作应记录详细日志，包括恢复时间、操作人员及数据版本信息。

7.3　数据加密存储

7.3.1　加密算法

7.3.1.1　静态数据存储应使用国家密码管理部门核准的加密算法。
7.3.1.2　密钥长度与加密模式宜符合行业安全标准，避免使用已公开漏洞的算法。

7.3.2　密钥管理

7.3.2.1　加密密钥应与数据分离存储，密钥管理系统应具备防泄露能力。
7.3.2.2　密钥生命周期应严格控制，超出有效期后宜自动轮换并销毁旧密钥。

7.3.3　细粒度加密

7.3.3.1　高敏感数据可采用字段级加密，仅授权用户可解密特定字段。
7.3.3.2　加密策略宜支持动态调整，适应数据分类分级变化需求。

7.4　访问控制

7.4.1　身份认证

7.4.1.1　数据访问请求方应通过多因素认证验证身份，如数字证书结合生物特征。
7.4.1.2　临时访问权限宜设置短时效，超时后自动失效。

7.4.2 权限管理

7.4.2.1 应基于角色或属性定义访问策略，遵循最小化授权原则。
7.4.2.2 权限变更时应即时生效，并通知数据所有者审核确认。

7.4.3 访问审计

7.4.3.1 所有数据访问操作应记录详细日志，包括访问时间、主体身份及操作类型。
7.4.3.2 审计日志宜采用防篡改技术存储，支持第三方审计机构查验。

7.5 数据完整性保障

7.5.1 校验机制

7.5.1.1 存储系统应定期计算数据哈希值，并与初始值比对验证完整性。
7.5.1.2 校验失败时，宜优先通过冗余副本修复数据，无法修复时应触发告警。

7.5.2 版本控制

7.5.2.1 关键数据应保留历史版本，版本数量宜根据业务需求与存储容量平衡。
7.5.2.2 版本回滚操作应经授权审批，并记录回滚前后的数据差异。

7.5.3 防篡改技术

7.5.3.1 存储系统可引入区块链技术，将数据哈希值锚定至链上实现防篡改。
7.5.3.2 数据修改操作应通过多方签名验证，确保变更行为合法可追溯。

7.6 存储生命周期管理

7.6.1 数据归档

7.6.1.1 低频访问数据宜迁移至归档存储层，降低主存储系统负载。
7.6.1.2 归档数据应保留元数据索引，支持快速检索与恢复。

7.6.2 数据销毁

7.6.2.1 销毁操作应覆盖存储介质物理层，确保数据不可恢复。
7.6.2.2 销毁过程应由独立监督方见证，并生成不可抵赖的销毁凭证。

7.6.3 容量规划

7.6.3.1 应建立存储容量预测模型，定期评估存储资源使用趋势。
7.6.3.2 扩容操作宜采用弹性伸缩策略，避免服务中断。

7.7 存储监控与审计

7.7.1 健康监控

7.7.1.1 应实时监控存储节点状态，包括磁盘利用率、I/O 性能及网络延迟。
7.7.1.2 监控数据宜可视化展示，支持异常阈值自定义告警。

7.7.2 安全审计

7.7.2.1 应定期对存储系统进行安全漏洞扫描，修复高风险漏洞。
7.7.2.2 审计范围应覆盖存储策略合规性、访问日志完整性及密钥管理有效性。
7.7.2.3 数据存储过程中应保障数据的安全性和合规性,应符合 GB/T 38633 有关规定。

7.7.3 性能优化

7.7.3.1 存储系统宜支持冷热数据分层管理，提升高频数据访问效率。
7.7.3.2 可启用缓存加速技术，减少跨域数据访问延迟。

8 运维监控与应急

8.1 实时告警机制

8.1.1 告警触发条件

8.1.1.1 应定义系统性能阈值、安全事件特征等告警触发规则。
8.1.1.2 告警规则宜支持动态调整，适应业务负载周期性变化。

8.1.2 告警分级与通知

8.1.2.1 告警事件应依据影响程度划分为紧急、高危、中危等级别。
8.1.2.2 紧急告警宜通过多通道同步通知责任人。

8.1.3 告警响应

8.1.3.1 接收到告警后，应在预设时间内启动应急响应流程。
8.1.3.2 告警处置过程应记录操作日志，并与原始告警信息关联存档。

8.2 应急响应流程

8.2.1 应依据事件类型划分应急场景，如数据泄露、服务中断、恶意攻击等。
8.2.2 宜针对每类场景制定标准化的处置预案，明确角色分工与操作步骤。
8.2.3 应优先隔离故障节点或异常流量，防止影响范围扩大。
8.2.4 涉及多域的应急事件，应启动跨域协同处置流程，共享事件情报。
8.2.5 处置完成后，宜生成事件分析报告并提交至跨域管理委员会审核。
8.2.6 应验证系统恢复后的功能完整性与数据一致性。
8.2.7 可启用备份数据或冗余节点快速重建业务环境。

8.3 日志与审计管理

8.3.1 应采集系统操作日志、安全事件日志及性能监控日志。
8.3.2 日志格式宜遵循标准化模板，确保跨域日志数据兼容性。
8.3.3 日志应集中存储并加密保护，保留期限不低于监管要求。
8.3.4 宜采用自动化分析工具识别日志中的异常模式，辅助根因定位。
8.3.5 应定期对日志进行合规性审计，检查是否存在违规操作。
8.3.6 审计结果宜作为跨域信任评级的参考依据。