ICS 35.240

CCS L 67

团 体 标 准

T/CQSI XXXX—2025

隐私计算 可信数据服务平台框架、功能及接口

Privacy-preserving computing

Trusted Data Service Platform Framework, Functions and Interfaces

（报批稿）

2025-XX-XX 发布 2025-XX-XX 实施

重庆市软件行业协会 发 布

目 次

[目 次 I](#_Toc202172031)

[前 言 III](#_Toc202172032)

[1 范围 1](#_Toc202172033)

[2 规范性引用文件 1](#_Toc202172034)

[3 术语及定义 1](#_Toc202172035)

[4 缩略语 2](#_Toc202172036)

[5 平台框架 2](#_Toc202172037)

[5.1 业务前端 2](#_Toc202172038)

[5.2 系统后端 3](#_Toc202172039)

[5.3 Web/Client 接口服务层 3](#_Toc202172040)

[6 基础功能 3](#_Toc202172041)

[6.1 业务前端功能设计 3](#_Toc202172042)

[6.1.1 隐私计算项目 3](#_Toc202172043)

[6.1.2 组件管理 3](#_Toc202172044)

[6.1.3 数据流通管理 3](#_Toc202172045)

[6.1.4 可信评估管理 3](#_Toc202172046)

[6.1.5 全周期存证溯源 3](#_Toc202172047)

[6.1.6 节点管理 3](#_Toc202172048)

[6.1.7 用户管理 3](#_Toc202172049)

[6.1.8 日志与审计 3](#_Toc202172050)

[6.2 系统后端模块设计 3](#_Toc202172051)

[6.2.1 数据资源管理 4](#_Toc202172052)

[6.2.2 基础密码库 4](#_Toc202172053)

[6.2.3 隐私计算引擎 4](#_Toc202172054)

[6.2.4 自适应选择 4](#_Toc202172055)

[6.2.5 联邦学习 4](#_Toc202172056)

[6.2.6 多方安全计算 4](#_Toc202172057)

[6.2.7 可信执行环境 4](#_Toc202172058)

[6.2.8 用户与授权 4](#_Toc202172059)

[6.2.9 通信传输 4](#_Toc202172060)

[6.2.10 扩展与集成 4](#_Toc202172061)

[6.2.11 日志与审计 4](#_Toc202172062)

[6.2.12 监控与可视化 4](#_Toc202172063)

[7 接口规范 4](#_Toc202172064)

[7.1 接口核心模块 4](#_Toc202172065)

[7.1.1 协议适配器 4](#_Toc202172066)

[7.1.2 路由网关 4](#_Toc202172067)

[7.1.3 安全认证 5](#_Toc202172068)

[7.2 接口协议规范 5](#_Toc202172069)

[7.2.1 数据传输格式 5](#_Toc202172070)

[7.2.2 接口版本管理 5](#_Toc202172071)

[7.3 安全控制要求 5](#_Toc202172072)

[7.3.1 通信加密 5](#_Toc202172073)

[7.3.2 访问控制 5](#_Toc202172074)

[7.3.3 审计日志 5](#_Toc202172075)

[7.3.4 限流防护 5](#_Toc202172076)

[7.4 接口安全规范 5](#_Toc202172077)

[7.4.1 认证流程 5](#_Toc202172078)

[7.4.2 敏感数据处理 6](#_Toc202172079)

[7.5 接口列表 6](#_Toc202172080)

[7.5.1 认证接口 6](#_Toc202172081)

[7.5.2 创建任务接口 6](#_Toc202172082)

[7.5.3 安全数据上传接口 7](#_Toc202172083)

[7.5.4 异步任务状态轮询接口 7](#_Toc202172084)

[8 安全与合规性 8](#_Toc202172085)

[8.1 数据安全 8](#_Toc202172086)

[8.2 合规性 8](#_Toc202172087)

[9 实施与维护 8](#_Toc202172088)

[9.1 部署要求 8](#_Toc202172089)

[9.2 维护与升级 8](#_Toc202172090)

[附 录 A 9](#_Toc202172091)

[A.1　基础相关标准 9](#_Toc202172092)

[A.2　技术相关标准 9](#_Toc202172093)

[A.3　服务相关标准 10](#_Toc202172094)

[A.4　管理相关标准 10](#_Toc202172095)

[附 录 B 11](#_Toc202172096)

[附 录 C 12](#_Toc202172097)

[C.1　创建隐私计算任务接口： 12](#_Toc202172098)

[C.2　安全数据上传接口（支持多方计算） 13](#_Toc202172099)

[C.3　异步任务状态轮询接口 14](#_Toc202172100)

[参 考 文 献 15](#_Toc202172101)

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。

本文件由重庆市软件行业协会提出并归口。

本文件起草单位：重庆市科学技术研究院、广州芳禾数据有限公司、杭州锘崴信息科技有限公司、北京理工大学、重庆邮电大学、济南超级计算技术研究院、西安交通大学、山东区块链研究院、中兴通讯股份有限公司、浙江大华技术股份有限公司、重庆市软件行业协会。

本文件主要起草人：熊黎丽、韩鹏、祝烈煌、沈俊宇、李明、侯锋、李智、孙琪、周由胜、张子剑、王亚杰、童瑶、左祥建、匡华龙、付勇、巫双果、孙怀义、张昊天、申博臣、陈怡同、杨和、蒋洪波、周扬眉、李国勇、刘巧、莫斌、刘谦、曹园、冯静荣、刘萃凡。

隐私计算可信数据服务平台框架、功能及接口

1 范围

本文件规定了隐私计算可信数据服务平台的框架、基础功能、接口规范、安全与合规性、实施与维护，适用于平台研发。

本文件适用于基于隐私计算的可信数据服务平台的研发、测试、实施及维护等。

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 25069-2022 信息安全技术 术语

GB/T 32905-2016 信息安全技术 SM3密码杂凑算法

GB/T 32907-2016 信息安全技术 SM4分组密码算法

GB/T 32918.1-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.3-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

GB/T 32918.4-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

GB/T 32918.5-2017 信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义

T/CCSA 406-2022 基于可信执行环境的数据计算平台技术要求与测试方法

T/CCSA 407-2022 基于多方安全计算的数据流通产品技术要求与测试方法

YD/T 4691-2024 隐私计算 联邦学习产品安全要求和测试方法

3 术语及定义

界定的以及下列术语和定义适用于本文件。

3.1

隐私计算 privacy-preserving computation

在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等信息流程全过程的各个环节中“可用不可见”。

注：隐私计算的常用技术方案有多方安全计算（Secure Multi-Party Computation）、联邦学习（Federated Learning）、可信执行环境（Trusted Execution Environment）等；常用的底层技术有混淆电路（Garbled Circuit）、不经意传输（Oblivious Transfer）、秘密分享（也称秘密分割，Secret Sharing）、同态加密（Homomorphic Encryption）等。

3.2

多方安全计算 secure multi-party computation

在一个分布式网络中，多个参与实体各自持有私密数据，各方希望以这些数据为输入共同完成对某函数的计算，而要求每个参与实体除计算结果、预期可公开的信息外均不能得到其他参与实体的任何输入信息。主要研究针对无可信第三方情况下，安全地进行多方协同的计算问题。

3.3

联邦学习 federated learning

一种多个参与方在保证各自原始私有数据不出数据方定义的可信域的前提下，以保护隐私数据的方式交换中间计算结果，从而协作完成某项机器学习任务的模式。

注：隐私数据包括原始私有数据、计算结果以及算法参数和模型参数中需要被保护的数据。算法参数和模型参数中需要被保护的数据根据实际应用场景确定，包括但不限于模型参数、梯度、样本分布等。隐私计算中的联邦学习不包含明文交换中间计算结果且未保护隐私数据的方案。

3.4

可信执行环境 trusted execution environment

数据计算平台上由软硬件方法构建的一个安全区域，可保证在安全区域内部加载的代码和数据在保密性和完整性方面得到保护。

3.5

SM2 密码算法 SM2 cryptographic algorithm

由 GB/T 32918（所有部分）定义的一种算法。

3.6

SM3 密码算法 SM3 cryptographic algorithm

由 GB/T 32905-2016 定义的一种算法。

3.7

SM4 密码算法 SM4 cryptographic algorithm

由 GB/T 32907-2016 定义的一种算法。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

FL：联邦学习（Federated Learning）

MPC：多方安全计算（Secure Multi-Party Computation）

SDK：软件开发工具包（Software Development Kit）

TEE：可信执行环境（Trusted Execution Environment）

5 平台框架

隐私计算可信数据服务平台通过分层架构设计，在确保数据隐私安全的前提下实现高效流通与协同计算。平台框架应分为业务前端、系统后端及Web/Client接口服务层三部分，如图1所示。基于隐私计算引擎、联邦学习（FL）、多方安全计算（MPC）及可信执行环境（TEE）等核心技术，结合数据资源管理与系统后端的安全监管能力，该平台起到保障数据隐私、实现跨领域可信数据流通并提升业务合规性的关键作用。整体架构通过这些模块的协作，推动隐私计算与安全计算技术在医疗、金融和政务领域的广泛应用。

图 1 隐私计算可信数据服务平台总体框架

5.1 业务前端

该层是面向平台管理者和业务用户的操作界面，提供隐私计算全生命周期的可视化管理和控制。其主要功能包括创建和管理隐私计算项目、组织和管理各类基础与应用组件、监控数据流通过程、进行可信评估、实现业务流程的全周期存证溯源、配置和管理平台节点、管理用户及其权限以及查看日志与审计信息。它封装了复杂的后台技术细节，为用户提供直观便捷的业务操作入口，是整个平台对外服务和管理的主要窗口。

5.2 系统后端

该层是平台的核心计算引擎和数据处理中枢，提供强大的数据处理、安全计算和监管能力。核心是隐私计算引擎​（支持自适应选择 FL / MPC / TEE 等技术），处理各类隐私计算任务。​数据资源管理模块负责数据的登记、接入、可信度量、权责界定、鉴权存证、存储及合规治理。此外，后端还提供基础支撑能力​（如节点发现与管理、容器加载、应用调度、加密通信、身份验证、访问控制）、安全监管能力​（如差分隐私保护、基础密码组件、密态计算框架、多种监管模型）、模型管理​（启停控制、聚合分发、版本控制）以及运维支撑​（API/SDK、日志记录、审计跟踪、参数监控）。它确保数据处理与计算过程安全可靠、合规可控，是平台隐私保护与数据价值释放能力的基石。

5.3 Web/Client 接口服务层

该层作为系统内外部的连接桥梁，提供统一的、标准化的交互接口​（Web API/Client SDK）。它衔接上层的行业应用（如医疗、金融、政务等场景的定制应用系统）与下层的业务前端和系统后端。此层实现了请求的路由转发、协议的转换适配（可能包括 RESTful API, gRPC, 消息队列等），并提供安全认证、加密通信、消息传递、多框架支持和插件机制等基础服务功能。其核心作用是简化行业应用集成，屏蔽后台技术复杂性，确保不同领域的外部应用能够安全、稳定、高效地调用平台的隐私计算服务和数据资源。

6 基础功能

6.1 业务前端功能设计

6.1.1 隐私计算项目

创建本地隐私计算项目及基于隐私计算技术（FL、MPC、TEE）开展的跨域数据协作任务，旨在实现数据可用不可见的目标，涵盖建模、分析及结果输出全流程。

6.1.2 组件管理

对隐私计算核心算法组件（FL、MPC、TEE）的封装、调度与版本控制，支持模块化扩展与动态替换。

6.1.3 数据流通管理

涵盖数据接入、存储、标注及治理功能，通过支持数据申请、权限审批、安全传输监控及全流程追踪，实现平台中数据在合规、可控、可追溯前提下的安全流通与协作。

6.1.4 可信评估管理

包含领域数据可信度量、共享平台可信度量、机构可信度量、隐私计算可信度量四个维度，保证数据来源可信、数据内容真实、数据价值可量化；保证平台所有者可信、平台使用可靠；保证接入机构/用户可信；保证隐私计算算法的性能、隐私泄露度、安全性可度量。

6.1.5 全周期存证溯源

记录数据从采集、计算到销毁的全链路操作日志，结合时间戳与哈希值固化技术，实现数据流转路径的可验证追溯。

6.1.6 节点管理

包含节点注册、节点信息（节点端口、IP地址、连接状态）等，以及服务器（CPU、GPU、内存使用）、磁盘使用率、网络带宽等。

6.1.7 用户管理

包含用户注册及权限管理（管理员、普通成员）、授权操作等。

6.1.8 日志与审计

用于记录、监控和分析系统活动和事件的关键机制，满足监管审查要求。

6.2 系统后端模块设计

平台系统应包括以下模块：

6.2.1 数据资源管理

建立覆盖数据全生命周期的系统化、规范化管理体系，通过数据分类分级、存储安全策略、精细化访问控制、灾备与恢复机制，以及动态合规监控，实现隐私计算平台中数据资源的规范存储、高效调用与安全可控，为业务前端数据流通管理模块提供合规、可信赖的数据服务支撑。

6.2.2 基础密码库

实现一套支持国密算法（SM2/SM3/SM4）、国际通用协议及行业定制化协议的标准化软件模块集合，提供加密、解密、签名验签、密钥全生命周期管理等核心功能，确保数据的机密性、完整性和可用性。

6.2.3 隐私计算引擎

支持多种隐私计算算法的执行，并提供统一的计算接口。

6.2.4 自适应选择

平台根据隐私计算的场景需求，硬件资源情况，数据特征等，通过自适应选择组件为隐私计算任务匹配最优算子/组件的组合。

6.2.5 联邦学习

从个性化数据、大规模数据、复杂共计场景等维度，实现高精、高效的安全联邦学习。

6.2.6 多方安全计算

从基础计算协议、机器学习算法、复杂攻击场景等维度，实现高效、抵抗多种威胁模型的多方安全计算。

6.2.7 可信执行环境

从状态信息缓存、完整性校验、本地和远程证明等维度，实现安全、自主可控、可扩展的可信执行环境。

6.2.8 用户与授权

信息安全体系中的核心组成部分，用于管理系统中用户的身份验证和权限分配。

6.2.9 通信传输

所有组件与其他节点的通信统一执行，发送/接收都通过注册到模块的方式按队列执行，信息发送时通过唯一标识从模块缓冲区中认领响应信息，满足FATE通信协议标准的规定。

6.2.10 扩展与集成

通过增加新功能或与其他系统、服务、工具进行连接，以增强现有系统的能力和适用范围。

6.2.11 日志与审计

用于记录、监控和分析系统活动和事件的关键机制。

6.2.12 监控与可视化

对系统、模型或流程的实时状态、性能指标和运行数据进行持续观测和记录，以确保其正常运行并及时发现异常。

7 接口规范

7.1 接口核心模块

7.1.1 协议适配器

支持RESTful API、gRPC、AMQP协议互转，转换延迟≤50ms。通过协议的转换，可以支持医疗、政务、金融等各领域的请求，把各种不同类型的请求转换成平台统一的接口请求方式。

7.1.2 路由网关

基于URL/消息头路由请求，支持负载均衡与故障转移。通过对适配后的HTTP请求进行限流或者JWT认证，保障后端服务的稳定性。

7.1.3 安全认证

集成OAuth 2.0客户端凭证流，支持JWT令牌校验。通过对请求进行校验，过滤掉不合法的请求，保障平台的接口数据安全。

7.2 接口协议规范

7.2.1 数据传输格式

 请求/响应体统一采用JSON格式，数据编码使用UTF-8编码。错误响应码遵循HTTP状态码标准（如400为错误的请求、503为服务不可用）。

7.2.2 接口版本管理

 版本号嵌入URL路径（如/v1.2/task/submit）。旧版本API需维护≥12个月。

7.3 安全控制要求

7.3.1 通信加密

全链路强制TLS 1.3加密，证书有效期≤1年。

7.3.2 访问控制

RBAC模型（角色：数据提供方/计算方/审计方），具体如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 角色​ | ​核心职能​ | ​权限范围​ | ​安全约束​ |
| 数据提供方​ | 提供原始数据 | 数据上传/加密 | 禁止访问计算结果；禁止修改他人数据（静态职责分离） |
| 数据元数据标注（如标签、分级） |
| 授权特定计算方使用数据 |
| 计算方​ | 执行隐私计算任务 | 发起计算任务 | 禁止访问原始数据；任务执行需数据方授权（动态职责分离） |
| 调用算法（如联邦学习、同态加密） |
| 获取加密结果 |
| 审计方​ | 监控与合规审查 | 查看操作日志 | 禁止参与数据/计算操作（角色互斥） |
| 审计数据使用记录 |
| 生成合规报告 |

表1 角色职能和权限范围

7.3.3 审计日志

记录接口调用方IP、用户ID、操作时间、参数摘要。

7.3.4 限流防护

按API Key限制QPS（默认100次/秒）。

7.4 接口安全规范

7.4.1 认证流程

业务系统根据预先分配的client\_id 和 secret 向认证服务请求 access\_token。在每次业务请求中，都在请求头部带上认证token，经由认证服务校验通过后，才将实际请求转发给平台核心。



图2 认证流程图

7.4.2 敏感数据处理

涉及数据标识的字段（如用户ID、医疗记录号）需进行HMAC-SHA256脱敏处理：
user\_id\_hashed = hmac\_sha256(salt, raw\_user\_id)。

7.5 接口列表

7.5.1 认证接口

|  |  |
| --- | --- |
| 属性 | 说明 |
| 接口名称 | 创建隐私计算任务 |
| 请求路径 | POST /oauth/token?client\_id=xx&secret=yy |
| 功能 | 认证用户是否合法，返回认证后的token |
| **输入参数：** |
| 路径参数 | client\_id 平台分配给各客户端的idsecret 平台分配给各客户端的secret |
| **输出参数​** | Json{"code": "200","data": {"access\_token": "eyJhb.....","expires\_in": 3600}}​状态码​：- 200：请求成功 |
| 安全控制 | 实际操作时，需要对secret 进行编码和签名操作 |

7.5.2 创建任务接口

|  |  |
| --- | --- |
| 属性 | 说明 |
| 接口名称 | 创建隐私计算任务 |
| 请求路径 | POST /v1/tasks |
| 功能 | 创建多方参与的隐私计算任务（如安全聚合、联合建模），并对敏感数据脱敏 |
| **输入参数：** |
| 请求头 | Authorization: Bearer <token>（JWT令牌） |
| 请求体 | Json{"algorithm": "PSI","dataId": "raw\_data\_123","parties": ["orgA", "orgB"]}​参数说明​：- algorithm：计算算法（如PSI、联邦学习）- dataId：原始数据标识- parties：参与方节点ID列表 |
| **输出参数​** | Json{"code": "201","data": {"taskId": "task\_20250618001","status": "TASK\_CREATED"}}​状态码​：- 200：创建成功- 403：权限不足（需DATA\_OWNER角色） |
| 安全控制 | 1. 敏感数据标识（dataId）需HMAC-SHA256脱敏处理2. 接口访问需数字签名认证 |

7.5.3 安全数据上传接口

|  |  |
| --- | --- |
| 属性 | 说明 |
| 接口名称 | 多方安全数据分片上传 |
| 请求路径 | POST /v1/data |
| 功能 | 上传数据并生成秘密共享分片，分布式存储至不同参与方 |
| **输入参数：** |
| 请求头 | Authorization: Bearer <token>（JWT令牌）Content-Type: multipart/form-data |
| 请求体 | - file：数据文件（二进制流）- data\_type：数据类型（仅支持DICOM/CSV） |
| **输出参数**​ | Json{"code": "200","data": {"status": "DATA\_READY","shares\_count": 3}}​参数说明​：- shares\_count：生成的分片数量 |

7.5.4 异步任务状态轮询接口

|  |  |
| --- | --- |
| 属性 | 说明 |
| 接口名称 | 异步任务状态轮询 |
| 请求路径 | GET /v1/tasks/{task\_id}/status |
| 功能 | 非阻塞轮询任务状态，支持自定义查询间隔 |
| **输入参数：** |
| 请求头 | Authorization: Bearer <token>（JWT令牌） |
| 路径参数 | task\_id：任务ID（例：task\_20250618001） |
| **输出参数**​ | Json{"code": "200","data": {"status": "SUCCESS","progress": 100%}}​状态值​：- PENDING：执行中- SUCCESS：成功- FAILED：失败（返回错误消息） |

8 安全与合规性

8.1 数据安全

平台应符合GB/T 35273-2020《个人信息安全规范》的要求。

平台应支持数据加密、脱敏和匿名化技术，确保数据隐私保护。

平台坚持数据保护三重目标：保密性、完整性和可用性。确保只有授权人员才能接触数据，同时防止数据被篡改，并保障合法用户随时使用数据。

平台坚持数据最小化原则，只收集必要的字段。同时对用途进行限定，明确告知数据使用范围。并控制数据生命周期，设置数据自动销毁规则。

8.2 合规性

平台应符合相关法律法规（如《个人信息保护法》）的要求。

平台应提供合规性审计报告，满足监管要求。

平台对法律进行责任映射，将法条分解为部门职责。审计保障机制保证证据链条完整，形成完整的操作记录，并引入第三方监督。

9 实施与维护

9.1 部署要求

平台应支持公有云、私有云和混合云部署模式。

平台技术厂商应提供详细的部署指南和技术支持，制定标准化手册和风险预案。

9.2 维护与升级

平台技术厂商应定期提供安全更新和功能升级，建立周全的补丁更新管理和版本更新演进机制。

平台技术厂商应支持平台的监控和故障排查，建立完善的故障应对机制，包括分级响应和知识沉淀，避免重复问题发生。

T/CCSA XXXX—XXXX

附 录 A

(资料性)

相关标准

A.1　基础相关标准

隐私计算基础相关标准见表A.1。

表A.1基础相关标准

| **标准类别** | **标准代码** | **标准名称** |
| --- | --- | --- |
| 隐私计算基础相关标准 | YD/T 4961.1-2024 | 隐私计算 跨平台互联互通 第1部分：总体框架 |
| YD/T 4961.2-2024 | 隐私计算 跨平台互联互通 第2部分：通信要求 |
| YD/T 4961.3-2024 | 隐私计算 跨平台互联互通 第3部分：互联协议 |
| YD/T 4961.4-2024 | 隐私计算 跨平台互联互通 第4部分：应用要求 |

A.2　技术相关标准

隐私计算技术相关标准见表A.2。

表A.2技术相关标准

| **标准类别** | **标准代码** | **标准名称** |
| --- | --- | --- |
| 术语相关标准 | GB/T 32400-2015 | 信息安全技术 云计算 概览与词汇 |
| GB/T 35295-2017 | 信息技术 大数据术语 |
| GB/T 25069-2022 | 信息技术 术语 |
| 算法相关标准 | GB/T 32905-2016 | 信息安全技术 SM3密码杂凑算法 |
| GB/T 32907-2016 | 信息安全技术 SM4分组密码算法 |
| GB/T 32918.1-2016 | 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则 |
| GB/T 32918.2-2016 | 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法 |
| GB/T 32918.3-2016 | 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议 |
| GB/T 32918.4-2016 | 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法 |
| GB/T 32918.5-2017 | 信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义 |
| 信息安全技术相关标准 | GB/T 20271-2006  | 信息安全技术 信息系统通用安全技术要求 |
| GB/T 38636-2020  | 信息安全技术 传输层密码协议（TLCP） |
| 产品相关标准 | YD/T 4947-2024 | 隐私计算 可信执行环境产品安全要求 |
| YD/T 4948-2024 | 隐私计算 可信执行环境产品性能测试要求 |
| YD/T 4690-2024 | 隐私计算 多方安全计算产品安全要求与测试方法 |
| YD/T 4690-2024 | 隐私计算 多方安全计算产品性能要求和测试方法 |
| YD/T 4691-2024 | 隐私计算 联邦学习产品安全要求与测试方法 |
| 应用相关标准 | JR/T 0196-2020  | 多方安全计算金融应用技术规范 |
| GB/T 39725-2020  | 信息安全技术 健康医疗数据安全指南 |
| T/ISC 0015-2022  | 金融场景隐私保护计算平台 |
| DB11/T 2049-2022 | 政务大数据安全技术框架 |
| TCCSA 472-2023  | 隐私计算应用 面向金融场景的应用要求 |
| DB54/T 0262-2024 | 政务信息数据共享交换平台技术规范 |
| TCCSA 473-2024 | 隐私计算应用 面向政务场景的应用要求 |

A.3　服务相关标准

隐私计算服务相关标准见表A.3。

表A.3服务相关标准

| **标准类别** | **标准代码** | **标准名称** |
| --- | --- | --- |
| 隐私计算相关服务标准 | GB/T 31168-2023 | 信息安全技术 云计算服务安全能力要求 |
| GB/T 35274-2023 | 信息安全技术大数据服务安全能力要求 |
| 个人信息服务相关标准 | GB/T 37964-2019 | 信息安全技术 个人信息去标识化指南 |
| GB/T 35273-2020 | 信息安全技术 个人信息安全规范 |

A.4　管理相关标准

隐私计算管理相关标准见表A.4。

表A.4管理相关标准

| **标准类别** | **标准代码** | **标准名称** |
| --- | --- | --- |
| 信息安全管理相关标准 | GB/T 22080-2016 | 信息技术 安全技术 信息安全管理体系 要求 |
| GB/T 22081-2024 | 网络安全技术 信息安全控制 |

附 录 B

（资料性）

标准统计表

隐私计算标准统计见表B.1。

表B.1标准统计表

| **标准一级类** | **标准二级类** | **合计** |
| --- | --- | --- |
| 基础标准 | 隐私计算基础相关标准 | 4 |
| 技术标准 | 术语相关标准 | 3 |
| 算法相关标准 | 7 |
| 信息安全技术相关标准 | 2 |
| 产品相关标准 | 5 |
| 应用相关标准 | 7 |
| 服务标准 | 隐私计算服务相关标准 | 2 |
| 个人信息服务相关标准 | 2 |
| 管理标准 | 信息安全管理相关标准 | 2 |
| 合计 | 34 |

附 录 C

(资料性)

接口标准

C.1　创建隐私计算任务接口：

|  |
| --- |
| Java@RestController@RequestMapping("/v1/tasks")public class TaskController { @Autowired private PrivacyComputeService computeService; @PostMapping public ResponseEntity<TaskResponse> createTask( @Valid @RequestBody TaskRequest request, @RequestHeader("Authorization") String token) {  // 身份验证与权限校验 AuthContext auth = authService.verifyToken(token); if (!auth.hasRole("DATA\_OWNER")) { throw new AccessDeniedException("权限不足"); } // 敏感数据脱敏处理（HMAC-SHA256） String hashedDataId = HmacUtils.sha256Hash(request.getDataId(), salt);  // 提交任务到隐私计算引擎 String taskId = computeService.submitTask( request.getAlgorithm(),  hashedDataId,  request.getParties() );  return ResponseEntity.status(HttpStatus.CREATED) .body(new TaskResponse(taskId, "SUBMITTED")); }} |

C.2　安全数据上传接口（支持多方计算）

|  |
| --- |
| Java@PostMapping("/v1/data")public DataUploadResponse uploadData( @RequestParam("file") MultipartFile file, @RequestParam("data\_type") String dataType) {  // 验证数据格式（示例：医疗影像数据） if (!Arrays.asList("DICOM", "CSV").contains(dataType)) { throw new InvalidDataException("不支持的数据类型"); } // 分片存储并生成秘密共享碎片 List<SecretShare> shares = SecretSharing.split( file.getBytes(),  3, // 总碎片数 2 // 最小恢复阈值 ); // 存储碎片到不同参与方 storageService.distributeShares(shares, "hospitalA", "researchB", "cloudC");  return new DataUploadResponse("DATA\_READY", shares.size());} |

C.3　异步任务状态轮询接口

|  |
| --- |
| Java@GetMapping("/v1/tasks/{task\_id}/status")public TaskStatus checkStatus( @PathVariable("task\_id") String taskId, @RequestParam(value = "poll\_interval", defaultValue = "5000") int interval) {  // 使用CompletableFuture非阻塞查询 return CompletableFuture.supplyAsync(() -> { while (true) { TaskStatus status = taskService.getStatus(taskId); if (status.isCompleted()) { return status; } Thread.sleep(interval); // 可配置轮询间隔 } }).exceptionally(ex -> new TaskStatus("FAILED", ex.getMessage()));} |

参 考 文 献

[1] GB/T 20985-2017 信息技术 安全技术 信息安全事件管理指南

[2] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

[3] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[4] GB/T 35273-2020 信息安全技术 个人信息安全规范

[5] GB/T 25069-2022 信息安全技术 术语

注：

本标准仅供参考，具体内容可根据实际情况进行调整。

本标准中涉及的隐私计算算法、数据安全技术等内容，可根据技术发展进行更新和补充。