ICS

 L

团 体 标 准

T/CCSA XXXX—XXXX

隐私计算 可信数据服务平台框架、功能及接口

Privacy-preserving computing

Framework, Functions and Interfaces of the Trusted Data Service Platform

（征求意见稿）

XXXX-XX-XX 发布 XXXX-XX-XX 实施

XXXXXXXXXXXXXXX 发 布

目 次

[前 言 III](#_Toc195079364)

[1 范围 1](#_Toc195079365)

[2 规范性引用文件 1](#_Toc195079366)

[3 术语及定义 1](#_Toc195079367)

[4 缩略语 2](#_Toc195079368)

[5 平台框架 2](#_Toc195079369)

[5.1 业务功能 3](#_Toc195079370)

[5.2 系统模块 3](#_Toc195079371)

[6 基础功能 3](#_Toc195079372)

[6.1 业务功能设计 3](#_Toc195079373)

[6.1.1 隐私计算项目 3](#_Toc195079374)

[6.1.2 组件管理 3](#_Toc195079375)

[6.1.3 数据资源管理 3](#_Toc195079376)

[6.1.4 数据权属管理 3](#_Toc195079377)

[6.1.5 可信评估管理 3](#_Toc195079378)

[6.1.6 全周期存证溯源 3](#_Toc195079379)

[6.1.7 节点管理 3](#_Toc195079380)

[6.1.8 用户管理 3](#_Toc195079381)

[6.1.9 日志与审计 3](#_Toc195079382)

[6.1.10 数据合规治理 3](#_Toc195079383)

[6.2 系统模块设计 3](#_Toc195079384)

[6.2.1 数据流通管理 3](#_Toc195079385)

[6.2.2 数据资源管理 3](#_Toc195079386)

[6.2.3 基础密码库 4](#_Toc195079387)

[6.2.4 隐私计算引擎 4](#_Toc195079388)

[6.2.5 自适应选择 4](#_Toc195079389)

[6.2.6 FL智能建模 4](#_Toc195079390)

[6.2.7 MPC隐私计算 4](#_Toc195079391)

[6.2.8 TEE 4](#_Toc195079392)

[6.2.9 用户与授权 4](#_Toc195079393)

[6.2.10 通信传输 4](#_Toc195079394)

[6.2.11 扩展与集成 4](#_Toc195079395)

[6.2.12 日志与审计 4](#_Toc195079396)

[6.2.13 监控与可视化 4](#_Toc195079397)

[7 接口规范 4](#_Toc195079398)

[7.1 组件接口规范 4](#_Toc195079399)

[7.1.1 数据输入输出接口 4](#_Toc195079400)

[7.1.2 算法接口 5](#_Toc195079401)

[7.1.3 安全控制接口 5](#_Toc195079402)

[7.1.4 可信度量接口 6](#_Toc195079403)

[7.1.5 消息通信接口 7](#_Toc195079404)

[7.1.5.1 消息发送接口 7](#_Toc195079405)

[7.1.5.2 回调函数接口 8](#_Toc195079406)

[8 安全与合规性 9](#_Toc195079407)

[8.1  数据安全 9](#_Toc195079408)

[8.2 合规性 9](#_Toc195079409)

[9 实施与维护 9](#_Toc195079410)

[9.1  部署要求 9](#_Toc195079411)

[9.2 维护与升级 9](#_Toc195079412)

[附 录 A 10](#_Toc195079413)

[A.1　基础相关标准 10](#_Toc195079414)

[A.2　技术相关标准 10](#_Toc195079415)

[A.3　服务相关标准 11](#_Toc195079416)

[A.4　管理相关标准 11](#_Toc195079417)

[附 录 B 12](#_Toc195079418)

[参 考 文 献 13](#_Toc195079419)

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、重庆邮电大学、北京理工大学、济南超级计算技术研究院、杭州锘崴信息科技有限公司、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。

本文件主要起草人：。

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的平台框架、基础功能、接口规范、安全与合规性和实施与维护。

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 20518-2018 信息安全技术 公钥基础设施 数字证书格式

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 32908-2016 非结构化数据访问接口规范

GB/T 32918-2016 信息安全技术 SM2椭圆曲线公钥密码法

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 35275-2017 信息安全技术 SM2密码算法加密签名消息语法规则

GB/T 35276-2017 信息安全技术 SM2密码算法使用规范

GB/T 35295-2017 信息技术 大数据 术语

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

T/ISC 0015-2022 金融场景隐私保护计算平台 技术要求与测试方法

3 术语及定义

GB/T 18794-2002、GB/T 32400-2015、GB/T 32908-2016、GB/T 35295-2017、GM/T 0002-2012、GM/T 0003.1-2012和GM/T 0004-2012界定的以及下列术语和定义适用于本文件。

3.1

隐私增强技术 privacy enhanced technology

是用于安全处理和共享敏感数据的技术。

注：隐私增强技术有两大类，即输入隐私增强技术和输出隐私增强技术。

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。

注：多方安全计算的常用技术有混淆电路（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。

[来源：T/CCSA 407-2022,3.1]

3.3

同态加密 homomorphic encryption

基于明文空间到密文空间同态性的公钥加密算法，计算方使用密文完成任务。

3.4

零知识证明 zero knowledge proof

是一种涉及两方或更多方的协议，证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄露任何关于被证明消息的信息。

3.5

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。

[来源：YD/T 4691-2024,3.1]

3.6

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。

[来源：T/CCSA 406-2022,3.1]

3.7

共识协议 consensus agreement

一种在分布式系统或区块链网络中，通过特定算法使多个参与方就某个决策达成一致的协议，确保数据的一致性和不可篡改性。

3.8

 差分隐私 differential privacy

 是一种用于解决隐私问题的隐私增强技术，以牺牲一定的数据准确度为代价，能够为用户数据提供严格的隐私保护。

4 缩略语

下列缩略语适用于本文件。

FL：联邦学习（Federated Learning）

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

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

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

SDK：软件开发工具包（Software Development Kit）

5 平台框架

隐私计算可信数据服务平台的框架应分为业务功能与系统模块两部分，如图1所示。



图 1 隐私计算可信数据服务平台总体框架

5.1 业务功能

业务功能是平台面向​​具体场景的解决方案。

5.2 系统模块

系统模块是平台的​​技术组件集合​​，负责提供隐私计算等业务功能所需的底层能力。

6 基础功能

6.1 业务功能设计

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智能建模、MPC隐私计算、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 数据资源管理

涵盖数据接入、存储、标注及治理功能，通过元数据管理、数据血缘追踪和数据质量校验，确保数据资源的可用性与合规性。

6.1.4 数据权属管理

通过区块链存证技术，明确数据所有权、使用权及收益权归属，支持数据流通中的权属验证与交易溯源。

6.1.5 可信评估管理

包含领域数据可信度量、共享平台可信度量、隐私计算可信度量三个维度，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；保证隐私计算算法的性能、隐私泄露度、安全性可度量。

6.1.6 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。

6.1.7 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。

6.1.8 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。

6.1.9 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。

6.1.10 数据合规治理

通过隐私影响评估、数据脱敏策略及动态合规检查，确保数据处理全流程符合法规要求。

6.2 系统模块设计

平台系统应包括以下模块：

6.2.1 数据流通管理

对数据在组织内部或跨组织之间的流动进行规划、控制、监控和优化的过程。

6.2.2 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，实现数据资产的高效利用、安全防护与价值释放。

6.2.3 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。

6.2.4 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。

6.2.5 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。

6.2.6 FL智能建模

一种分布式机器学习范式，在不转移原始数据的前提下，通过多方协同训练全局模型，保护数据隐私。

6.2.7 MPC隐私计算

多个参与方共同对输入数据进行计算，输出结果的同时确保各方输入数据的隐私性(即不泄露各自输入)。

6.2.8 TEE

基于硬件安全的 CPU 实现基于内存隔离的安全计算，可在保证计算效率的前提下完成隐私保护的计算。

6.2.9 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。

6.2.10 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。

6.2.11 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。

6.2.12 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。

6.2.13 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 组件接口规范

组件接口设计的目标是确保各组件可以快速、高效地接入平台并与其他组件进行交互。接口规范包括数据输入/输出接口、算法接口、安全控制接口和可信度量接口。

7.1.1 数据输入输出接口

用于数据的输入和输出，确保数据能够在组件之间顺畅流通。

接口定义：

|  |
| --- |
| ProtoBufservice DataProcessor { rpc ProcessData (DataRequest) returns (DataResponse) {}}message DataRequest { string userId = 1; string data = 2;}message DataResponse { string result = 1;} |

7.1.2 算法接口

用于调用具体的隐私计算算法，包括算法参数配置和执行控制。

接口定义：

|  |
| --- |
| ProtoBufservice FederatedLearning { rpc Execute (FederatedLearningRequest) returns (FederatedLearningResponse) {}}message FederatedLearningRequest { float learningRate = 1; int32 numIterations = 2; repeated string data = 3;}message FederatedLearningResponse { string result = 1;} |

7.1.3 安全控制接口

用于定义数据的加解密和权限管理等安全控制操作。

接口定义：

|  |
| --- |
| ProtoBufservice SecurityControl { rpc EncryptData (DataRequest) returns (DataResponse) {} rpc DecryptData (DataRequest) returns (DataResponse) {} rpc Authorize (AuthorizeRequest) returns (AuthorizeResponse) {}}message DataRequest { string data = 1;}message DataResponse { string encryptedData = 1; string data = 2;}message AuthorizeRequest { string user = 1; string operation = 2;}message AuthorizeResponse { bool isAuthorized = 1;} |

7.1.4 可信度量接口

用于定义数据、平台及隐私计算过程的可信度量方法。

接口定义：

|  |
| --- |
| ProtoBufservice TrustMeasurement { rpc MeasureDataTrust (DataRequest) returns (TrustResponse) {} rpc MeasurePlatformTrust (PlatformRequest) returns (TrustResponse) {} rpc MeasureComputationTrust (ComputationRequest) returns (TrustResponse) {}}message DataRequest { string data = 1;}message PlatformRequest { string platform = 1;}message ComputationRequest { string process = 1;}message TrustResponse { float trustScore = 1;} |

7.1.5 消息通信接口

所有组件的发送和接收都通过消息分发模块按队列执行，信息发送时通过唯一标识从模块缓冲区中认领响应信息，并通过回调函数通知组件，确保消息的顺序性和一致性。

7.1.5.1 消息发送接口

用于组件向其他节点发送消息，消息通过消息分发模块进行处理。

接口定义：

|  |
| --- |
| ProtoBufsyntax = "proto3";service MessageDispatcher { rpc SendMessage (MessageRequest) returns (MessageResponse) {}}message MessageRequest { string sender = 1; string receiver = 2; string job\_id = 3; string data\_id = 4; string request\_id = 5; string timestamp = 6; string payload = 7; string callbackEndpoint = 8; // 回调函数的gRPC端点}message MessageResponse { string request\_id = 1; string status = 2; // 状态，如 "sent", "error"} |

7.1.5.2 回调函数接口

用于组件接收来自消息分发模块的响应消息。

接口定义：

|  |
| --- |
| ProtoBufservice CallbackHandler { rpc OnMessageReceived (CallbackRequest) returns (CallbackResponse) {}}message CallbackRequest { string request\_id = 1; string payload = 2;}message CallbackResponse { string status = 1; // 状态，如 "received", "error"} |

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。

支持数据加密、脱敏和匿名化技术，确保数据隐私保护。

8.2 合规性

平台应符合相关法律法规（如GDPR、CCPA）的要求。

提供合规性审计报告，满足监管要求。

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。

提供详细的部署指南和技术支持。

9.2 维护与升级

提供定期的安全更新和功能升级。

支持平台的监控和故障排查。

T/CCSA XXXX—XXXX

附 录 A

(规范性)

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** | **标准编号** | **标准代码** | **标准名称** |
| --- | --- | --- | --- |
| 隐私计算基础相关标准（B12） | B1201 | YD/T 4961.1-2024 | 隐私计算 跨平台互联互通 第1部分：总体框架 |
| B1202 | YD/T 4961.2-2024 | 隐私计算 跨平台互联互通 第2部分：通信要求 |
| B1203 | YD/T 4961.3-2024 | 隐私计算 跨平台互联互通 第3部分：互联协议 |
| B1204 | 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** | **标准编号** | **标准代码** | **标准名称** |
| --- | --- | --- | --- |
| 术语相关标准（B21） | B2101 | GB\_T 25069-2022 | 信息安全技术 术语 |
| B2102 | GB\_T 35295-2017 | 信息技术 大数据术语 |
| B2103 | GB\_T 32400-2015 | 信息技术 云计算概览与词汇 |
| 算法相关标准（B22） | B2201 | GM\_T 0003.1-2012  | SM2椭圆曲线公钥密码算法 第1部分：总则 |
| B2202 | GM\_T 0003.2-2012  | SM2椭圆曲线公钥密码算法 第2部分：数字签名算法 |
| B2203 | GM\_T 0003.3-2012  | SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议 |
| B2204 | GM\_T 0003.4-2012  | SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法 |
| B2205 | GM\_T 0004-2012  | SM3密码杂凑算法 |
| B2206 | GM\_T 0002-2012  | SM4分组密码算法 |
| 信息安全技术相关标准(B23) | B2301 | GB\_T 20271-2006  | 信息安全技术 信息系统通用安全技术要求 |
| B2302 | GB\_T 38636-2020  | 信息安全技术 传输层密码协议（TLCP） |
| 产品相关标准（B24） | B2401 | YD/T 4947-2024 | 隐私计算 可信执行环境产品安全要求 |
| B2402 | YD/T 4948-2024 | 隐私计算 可信执行环境产品性能测试要求 |
| B2403 | 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 |
| B2404 | 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 |
| B2405 | 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(B25) | B2501 | T/ISC 0015-2022  | 金融场景隐私保护计算平台 |
| B2502 | TCCSA 472-2023  | 隐私计算应用 面向金融场景的应用要求 |
| B2503 | JR\_T 0196-2020  | 多方安全计算金融应用技术规范 |
| B2504 | DB11\_T 2049 | 政务大数据安全技术框架 |
| B2505 | DB54\_T 2024 | 政务信息数据共享交换平台技术规范 |
| B2506 | TCCSA 473-2024 | 隐私计算应用 面向政务场景的应用要求 |
| B2507 | GBT 39725-2020  | 信息安全技术 健康医疗数据安全指南 |

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** | **标准编号** | **标准代码** | **标准名称** |
| --- | --- | --- | --- |
| 隐私计算相关服务标准（B32） | B3201 | GB\_T 35274-2023 | 信息安全技术 大数据服务安全能力要求 |
| B3202 | GB\_T 31168-2014  | 信息安全技术 云计算服务安全能力要求 |
| 个人信息服务相关标准(B33) | B3301 | GB\_T 35273-2020 | 信息安全技术 个人信息安全规范 |
| B3302 | GB\_T 37964-2019  | 信息安全技术 个人信息去标识化指南 |

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** | **标准编号** | **标准代码** | **标准名称** |
| --- | --- | --- | --- |
| 信息安全管理相关标准（B42） | B4201 | GB\_T 22080-2008  | 信息技术 安全技术 信息安全管理体系 要求 |
| B4202 | GB\_T 22080-2008 | 信息技术 安全技术 信息安全管理实用规则 |

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** | **相关标准数量** | **合计** |
| --- | --- | --- | --- |
| 基础标准 | 隐私计算基础相关标准 | 4 | 4 |
| 技术标准 | 术语相关标准 | 3 | 3 |
| 算法相关标准 | 6 | 6 |
| 信息安全技术相关标准 | 2 | 2 |
| 产品相关标准 | 5 | 5 |
| 应用相关标准 | 7 | 7 |
| 服务标准 | 隐私计算服务相关标准 | 2 | 2 |
| 个人信息服务相关标准 | 2 | 2 |
| 管理标准 | 信息安全管理相关标准 | 2 | 2 |
| 合计 | 33 | 33 |

参 考 文 献

[1] GB/T 35273-2020 信息安全技术 个人信息安全规范

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

[3] GB/T 25069-2010 信息安全技术 术语

[4] GB/T 32918-2016 信息技术 安全技术 信息安全事件管理指南

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

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。