TC609

全国数据标准化技术委员会技术文件

TC609-6-2026-XX

数据基础设施 隐私保护计算公共服务平台

Data infrastructure – Public service platform of privacy-preserving computation

（征求意见稿）

2026-XX-XX 发布　　2026-XX-XX 实施

全国数据标准化技术委员会　发布

目　　次

前　言

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。
本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。
本文件起草单位：

数据基础设施 隐私保护计算公共服务平台

1 范围

本文件规范了隐私保护计算公共服务平台作为数据基础设施公共支撑能力组件的部署方式、数据服务能力、功能架构、接入方式、互通和安全要求。

本文件适用于适用于隐私保护计算公共服务平台的设计、建设、运营，以及连接器的接入与协同，为平台开发者、使用者和第三方评估机构提供参考。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

隐私保护计算 privacy-preserving computation

在保证数据提供方不泄露原始数据（3.6）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、销毁等数据流转全过程的各个环节中“可用不可见”。

注：隐私保护计算的常用技术方案有安全多方计算、联邦学习、可信执行环境、密态计算等；常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

[来源：数据领域常用名词解释（第一批）]

3.2

隐私保护计算公共服务平台 common service platform of privacy-preserving computation

运用隐私保护计算技术，统筹利用计算资源、存储资源、网络资源、信息资源、应用支撑等资源，以公共服务的形式为数据基础设施相关节点和参与方提供隐私保护计算能力组件式服务的平台。

3.3

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源：GB/T 25069—2022，定义 3.41]

3.4

系统 system

为实现一个或多个既定目的而组织起来的相互作用元素的组合。

[来源：GB/T 25069:2022，定义 3.648]

3.5

参与方 party

参与隐私保护计算的自然人或法人。

[来源：GB/T 32400—2015，3.1.6，有修改]

3.6

原始数据 raw data

隐私保护计算任务中，数据提供方提供的输入信息。

3.7

密态计算 cryptographic computing

通过综合利用密码学、可信硬件和系统安全相关技术，实现计算过程数据可用不可见，计算结果能够保持密态化，以支持构建复杂组合计算，实现计算全链路保障，防止数据泄漏和滥用。

[来源：数据领域常用名词解释（第一批）]

3.8

敏感数据 sensitive data

由参与方确定的受保护的信息数据。

注：敏感信息数据的泄露、修改、破坏或丢失对人或事产生可预知的损害。

[来源：GB/T 39477—2020，3.7，有修改]

3.9

数据处理 data processing

包括数据的收集、存储、使用、加工、传输、提供、公开等活动。

[来源：数据领域常用名词解释（第一批）]

4 缩略语

下列缩略语适用于本文件。

GPU：图形处理器（Graphics Processing Unit）

JSON：JavaScript对象表示法（JavaScript Object Notation）

OCI：开放容器倡议（Open Container Initiative）

SQL：结构化查询语言（Structured Query Language）

5 概述

本小节从多个角度，对隐私保护计算的内涵外延、技术特征及其在数据基础设施中的实现路径进行概要阐述。

从概念角度，隐私保护计算是一类在保障数据提供方原始数据不出域和不泄露的前提下，实现数据可用不可见的技术体系，其核心目标是破解数据要素流通中安全与利用的矛盾，确保数据在产生、存储、计算、应用、销毁全生命周期中满足保密性、完整性与可用性要求，为跨主体、跨域数据安全融合与价值释放提供技术信任的支撑。

从技术角度，隐私保护计算包含了丰富的技术栈，包含安全多方计算、联邦学习、可信执行环境、密态计算等为主干技术路径，底层依托混淆电路、不经意传输、秘密分享、同态加密等密码学通过算法组件标准化封装（如PSI、联合统计、隐匿查询等），支持数据分析、联合建模、密态推理等场景化服务。

从系统角度，隐私保护计算公共服务平台提供安全可信的数据融合加工服务，其核心在于保障原始数据不出域的前提下实现可用不可见，有效防范内外部非授权主体对数据的窃取或滥用。面向数据提供方，平台为其提供自主控制数据使用的权限，确保数据在流转过程中的保密性、完整性与可用性；同时，平台保障仅授权方能按约定方式获取计算结果，有效防止未授权访问与数据滥用。依托多元的技术路线和灵活部署模式，平台支持按业务场景实施分级策略，在保障安全的同时兼顾业务效率。

在与数据基础设施关系方面，隐私保护计算公共服务平台是国家数据基础设施中的公共支撑能力组件，为数据基础设施中相关节点和参与方提供基于隐私保护计算技术的公共服务能力。平台可以复用数据基础设施统一身份、目录、标识体系，支持“平台集中计算”“平台-连接器协同”等灵活计算模式，为数据流通利用提供隐私保护计算能力支撑。

6 定位

隐私保护计算公共服务平台作为国家数据基础设施中的公共支撑能力组件，平台以公共服务形式提供普惠化的隐私保护计算能力，集中实现算力供给、算法组件管理、隐私保护计算能力支撑等能力，应符合《20255408-T-907数据基础设施 参考架构》（征求意见稿）确定的国家数据基础设施整体架构及基本约束，并继承国家数据基础设施业务节点基本要求,如图1所示。

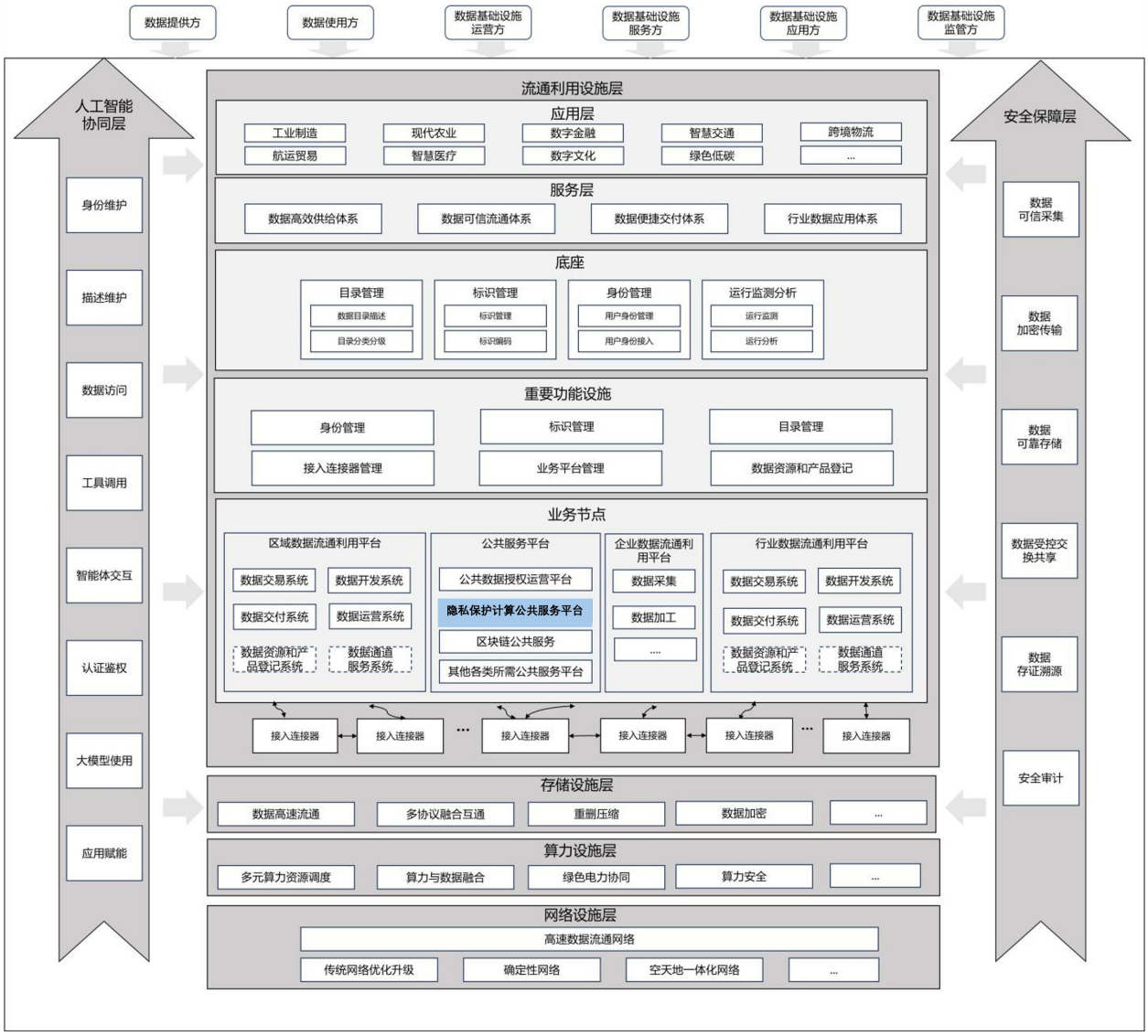

图 1　隐私保护计算公共服务平台在数据基础设施中的位置

7 部署方式

隐私保护计算公共服务平台和接入连接器之间支持以下一种或多种计算模式，如图 2 所示：

集中式部署：多个接入连接器分别上传加密的数据至隐私保护计算公共服务平台。公共服务平台接收加密数据后，执行相应的隐私保护计算任务，如任务#1、任务#2 等；

混合式部署：隐私保护计算公共服务平台和具备隐私保护计算能力的接入连接器之间进行交互执行隐私保护计算任务。此外，平台还提供了算法组件、调度等支持；

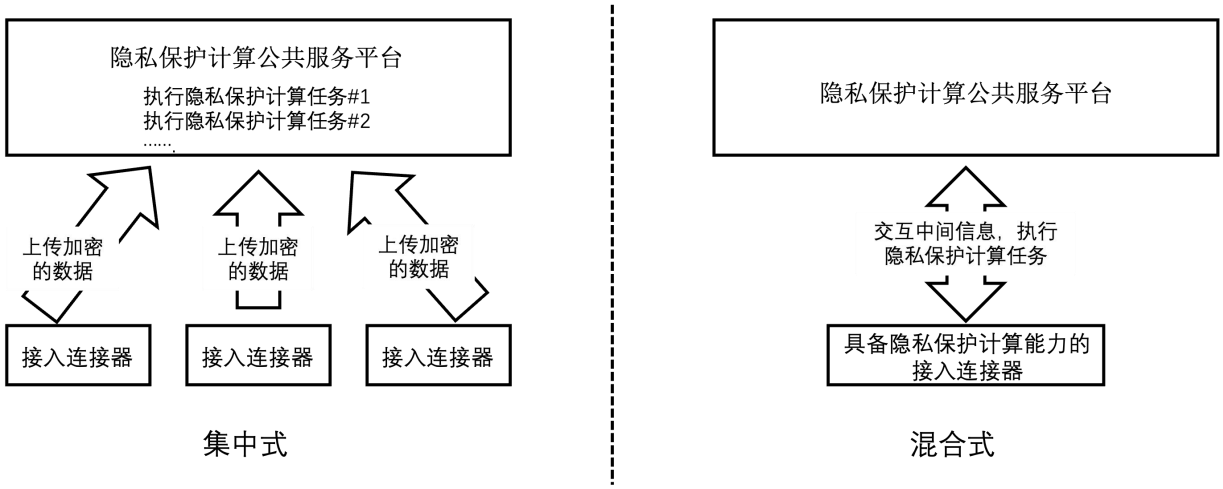

图 2　隐私保护计算公共服务平台和接入连接器间的部署模式

8　服务能力

8.1　概述

典型的数据服务包括数据分析、建模服务和推理服务，如附录A所示。

8.2　数据分析服务

隐私保护计算公共服务平台为用户提供数据分析服务，包含但不限于：

a）　隐私集合求交。在确保多个数据提供方数据集安全的前提下，执行集合求交操作。该服务仅计算并输出数据集之间的共同数据记录，保护交集之外的数据信息不被泄露或滥用；

b）　联合统计。在保障多个数据提供方数据集安全的前提下，执行联合统计分析操作。该服务支持 SQL、Python 等计算脚本，实现多个数据集的统计计算，包括但不限于均值、中位数、标准差、相关性分析等统计指标，确保各方原始数据在统计过程中不被泄露或滥用；

c）　隐匿查询。隐私保护计算公共服务平台为用户提供隐匿查询服务，应允许用户在不泄露查询内容的前提下，从数据集中检索特定信息；

d）　分析结果密态交付。数据分析结果应支持通过双方约定的方式交付给数据使用方，包括但不限于 API 接口调用、数据报告生成。对于高敏感高价值推理结果，宜支持数据分析结果的密态交付，即只有授权的使用方能够在安全的环境下使用数据，避免结果落地后失控。

8.3　建模服务

隐私保护计算公共服务平台为用户提供联合建模服务。该服务在保障各数据提供方数据集安全的前提下，多方协作执行建模操作。联合建模服务包含但不限于：

a）　算法支持。支持主流机器学习算法的联合建模，包括但不限于树模型、逻辑回归等；

b）　多样化数据集分布。支持不同数据集分布模式下的联合建模，包括用户群体相同但特征信息互补的数据集分布场景，以及用户群体不同但特征维度相似的数据集分布场景；

c） 应支持保护中间数据。支持对联合建模过程中的中间数据（如模型梯度、损失函数、参数更新等）进行保护，防止中间数据泄露或被恶意利用推断原始数据；

d） 模型交付管理。支持多种模型交付方式，确保模型结果按照预定方式交付给授权参与方。支持单一参与方获得完整模型或各参与方获得模型分片。支持不直接交付模型参数，通过 API 接口提供模型推理服务。

8.4 推理服务

隐私保护计算公共服务平台为用户提供数据推理服务，包含但不限于：

a） 模型部署保护。支持用户将推理模型安全部署在平台上，确保模型参数的完整性和保密性；

b） 样本数据保护。支持用户输入待预测样本，平台采用可信执行环境、同态加密等隐私保护计算技术，确保待预测样本在推理过程中的完整性和保密性；

c） 大模型推理服务。在大模型推理服务过程中，平台宜提供与非隐私保护计算框架（如 Pytorch、vllm 等）对等的接口，以保护模型 IP、推理交互信息等，防止被泄露或模型盗用；

d） 推理结果交付。支持推理结果加密后以API接口、文件传输、数据库对接等在线或离线方式交付给数据使用方，确保只有数据使用方能解密并使用结果。

9 功能架构

9.1 概述

隐私保护计算公共服务平台是数据基础设施中的公共服务组件，包含算法组件管理、数据服务辅助、管理与审计、隐私保护计算技术和基础软硬件环境，如图3所示。

管控与审计模块包括隐私保护计算公共服务平台的权限管控和存证审计的能力。数据服务辅助为数据流通参与方提供数据流通相关的服务，如数据接入、随机数服务、任务协商等。算法组件管理协助数据提供方、使用方完成隐私保护计算算法的协商及调用。隐私保护计算技术和基础软硬件环境模块分别提供隐私保护计算技术能力支持和底层算力与运行环境，包括支持安全地计算所需的CPU、GPU和NPU等硬件资源及相关系统软件。

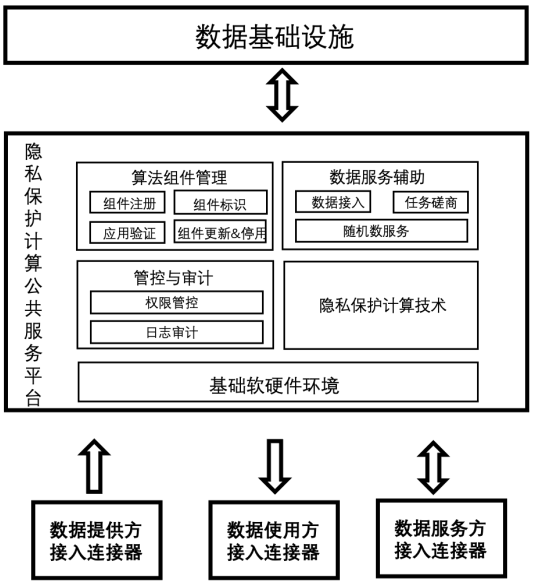

图 3 隐私保护计算公共服务平台架构图

9.2 算法组件管理

隐私保护计算公共服务平台支持算法组件管理的基本功能，协助数据提供方、使用方完成隐私保护计算算法的协商及使用，应包含以下功能：

a) 算法组件注册：通过权威机构安全性测试的隐私保护计算算法并且具有权威机构对算法的签名，可由算法提供方登记至隐私保护计算公共服务平台，供数据提供方与使用方检索和选用；
b) 算法组件标识：平台对上传算法进行完整性验证后分配在隐私保护计算公共服务平台上唯一标识，供数据提供方与使用方检索、比对与调用；
c) 应用验证：支持数据提供方等参与方对算法进行远程验证，判断其运行逻辑是否符合预期；
d) 算法组件更新：平台为已注册算法提供更新，算法提供方可在线提交新版本镜像，在平台上生成新的版本号与内容哈希。算法组件更新应不影响已签署合约的任务；
e) 算法组件停用：算法提供方发起停用申请，或算法被发现存在重大漏洞时，平台将该算法置为停用状态，停止调度并冻结镜像下载。对已启动任务可以发起停止任务。

9.3 数据服务辅助

9.3.1 数据接入

隐私保护计算公共服务平台提供数据接入服务：

a) 平台支持接入数据的元数据信息，元数据中需明确说明支持的隐私保护计算算法类型及其应用场景；
b) 支持通过对象存储、数据库等服务接入加密后的数据且保持密态的状态下托管在平台上。

9.3.2 任务磋商

隐私保护计算公共服务平台提供任务磋商服务：

a) 支持数据使用方和数据提供方通过平台进行隐私保护计算任务协商，支持双方就算法组件、参数配置、结果交付方式等进行协商确认；
b) 支持按照协商确定的参数和策略执行隐私保护计算任务，并提供任务状态监控和异常处理机制。

9.3.3 随机数服务

隐私保护计算公共服务平台提供满足一定相关性的随机数，如提供一组随机数 $\boldsymbol{a}$, $\boldsymbol{b}$ 和 $\boldsymbol{c}$,满足$\boldsymbol{c} = \boldsymbol{a} \times \boldsymbol{b}$。随机数需要通过安全的通信渠道分发给参与计算的各方，防止随机数在传输过程中被截获或篡改，可用于优化安全多方计算加法、乘法等运算，提高隐私保护计算的执行效率。

9.4 管控与审计

9.4.1 权限管控

隐私保护计算公共服务平台具有权限管控功能，包括但不限于如下的权限管控：

a) 角色身份：应支持定义多类角色身份，并支持按类分配不同的权限；
b) 权限设置：应支持针对不同数据和应用服务定义具体的可见权限、访问权限和操作权限，对于已授权的开放资源，支持数据拥有方关闭数据授权；
c) 权限审核：支持权限审核功能，定期检查和审计用户权限配置，防止权限滥用和权限泄露；
d) 使用授权：数据加工使用的授权应由所属的数据提供方生成或者以数据提供方认可的方式生成，应确保授权的真实性和完整性，平台方不能伪造；
e) 授权内容：授权的内容应包含但不限于数据、使用范围、使用对象、加工使用策略和授权有效期等；
f) 使用鉴权：在数据加工使用、访问前，应进行鉴权操作；
g) 鉴权过程：鉴权操作应具有完整的校验链条，包含但不限于请求身份、数据信息、数据提供方签名、使用策略等。应确保授权信息是由真实的数据提供方签发的且数据的请求内容和授

权内容是一致。当授权、鉴权操作是计算方平台或第三方提供时，要保证授权、鉴权操作不能被平台或第三方的内容人员伪造、篡改或绕过。

9.4.2 日志审计

隐私保护计算公共服务平台宜按需复用其他业务节点中的日志审计相关功能，也可在平台中集成日志审计功能，允许隐私保护计算公共服务运营方记录业务执行、系统运行的日志，并提供审计服务。隐私保护计算公共服务平台日志审计功能应采用传统的权威第三方存证，也可结合时间戳、数字签名和证书、哈希校验、可信计算等技术，强化数据存证的可信。日志审计应包含如下功能：

a) 日志存证：应对数据接入、研发、分析和建模等数据服务全流程中数据处理动作、权限管理和人员操作等进行记录；
b) 日志内容：应包括但不限于时间、事件主体、事件客体、事件描述、事件结果等；
c) 日志留存：日志保留时间应符合根据数据安全等级相关标准规定；
d) 日志查验：支持对已存证日志的查询、验证；
e) 审计追溯：提供日志存证信息进行审计溯源、合规检查，支持隐私保护计算公共服务平台监管方对平台运行情况进行监管。支持相关方对数据使用控制是否符合数字合约约束进行审计。

9.5 隐私保护计算技术

隐私保护计算公共服务平台应支持以下隐私保护计算技术中的至少 4 种：

a) 安全多方计算：支持多个参与方在不直接暴露各自的私有数据的情况下，共同完成对某函数的计算。每个参与方除计算结果、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；
b) 可信执行环境：具备硬件级隔离及安全启动机制，为数据服务的保密性、完整性、真实性和不可否认性提供了运行环境，进一步结合密钥、身份等方面的管控机制实现数据流通保障；
c) 密态计算：通过综合利用密码学、可信硬件和系统安全相关技术，实现计算过程数据可用不可见，计算结果能够保持密态化，以支持构建复杂组合计算，实现计算全链路保障，防止数据泄露和滥用；
d) 联邦学习：支持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，实践中需要重点关注中间数据结果的保护；
e) 同态加密：允许对密文进行计算操作并产生加密结果，这些结果在解密后与原数据进行同样操作的结果相同；
f) 其它：根据业务需要，支持零知识证明、差分隐私等隐私保护计算技术。

9.6 基础软硬件环境

隐私保护计算公共服务平台基础软硬件环境层提供安全可信的计算环境，结合加速设备，为数据服务提供密态算力资源：

a) 应支持构建安全、隔离的计算环境，确保数据在计算过程中的保密性与完整性；
b) 应支持集群管理，对集群内的可信计算环境单元进行统一管理和调度，保障各单元的安全性和协同工作能力；
c) 可在加速设备（如 GPU、NPU）层面构建安全隔离环境，保护加速设备核心计算过程中的敏感数据（如模型参数、训练样本），还需保障 CPU 与 GPU 之间、多 GPU 之间的数据传输链路安全，防止侧信道攻击和跨设备数据泄露。

10 交互关系

10.1 概述

集中式的部署模式，参与方将加密的数据上传至隐私保护计算公共服务平台。参与方通过接入连接器与隐私保护计算公共服务平台的接入连接器对接，实现加密后的数据传输，传输完成后在平台操作发起隐私保护计算任务。

混合式部署模式，参与方需要平台保持交互联合进行隐私保护计算任务，隐私保护计算公共服务平台和接入连接器之间需要通过组件和应用管理、环境互通和任务互通的交互接口进行交互，交互接口示意图如图 4 所示。组件和应用管理、环境互通和任务互通的接口要求见 10.2、10.3、10.4 章节。

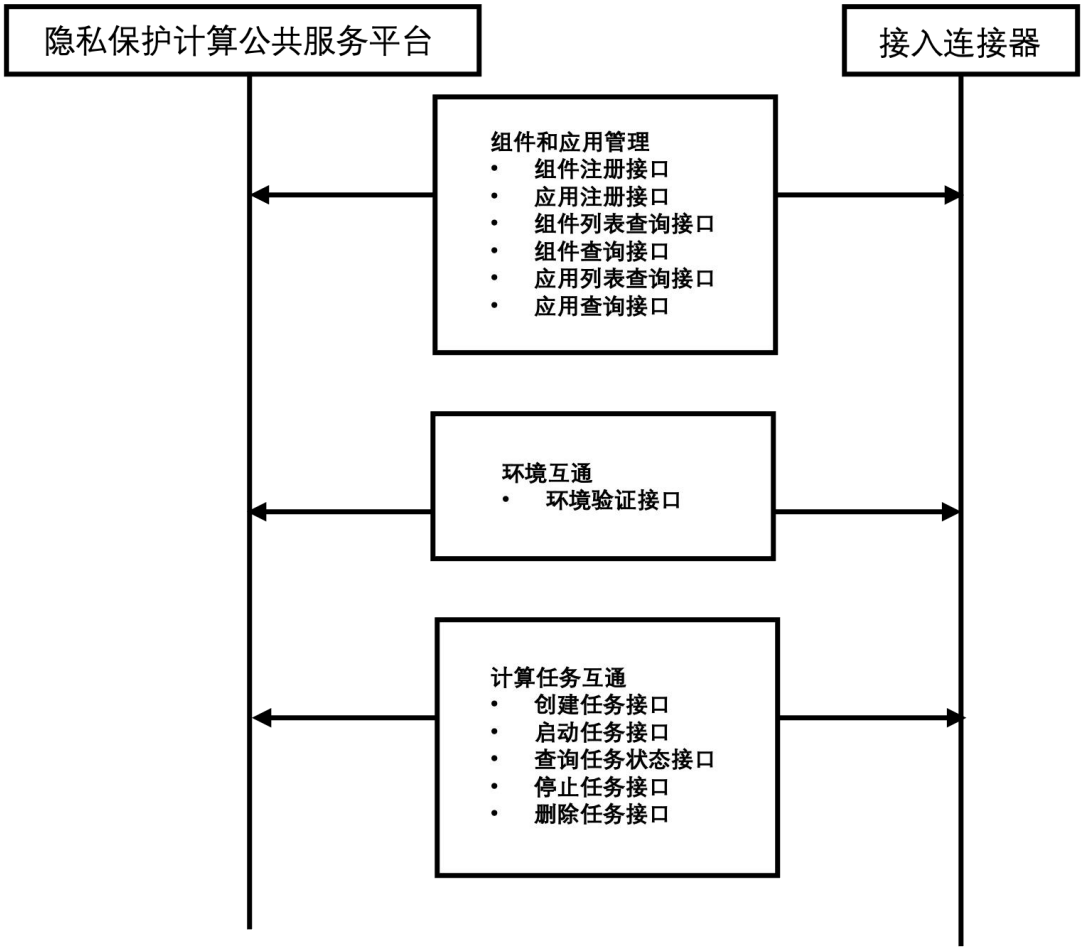

图 4　隐私保护计算公共服务平台和接入连接器间的交互接口示意图

10.2　组件和应用管理

隐私保护计算算法组件是将隐私保护计算中的单个算法能力进行标准化封装后形成的最小可执行单元。它通常包含算法实现代码、运行所需的镜像/依赖、输入输出数据定义、参数（超参）描述、资源与运行环境约束，以及可复用的接口规范，使组件能够被调度系统调用与编排。基于隐私保护计算的数据服务应用是面向具体业务目标，由一个或多个算法组件按顺序或拓扑关系组合编排形成的可交付执行体。应用不仅描述组件之间的数据流与控制流关系，还包含全局与组件级参数配置、运行时策略（如重试、并发、容错）、以及部署所需的基础设施封装（例如虚拟机/容器规格、网络与端口、存储挂载、配置模板与密钥注入等），从而支持应用在目标环境中一键部署、统一运维与版本管理。隐私保护计算公共服务平台支持参与方注册和查询隐私保护计算组件和应用，如附录B所示，应包含以下接口：

a） 组件注册接口：接入连接器或其它业务节点通过该接口在平台上注册隐私保护计算算法组件；

b） 应用注册接口：接入连接器或其它业务节点通过该接口在平台上注册隐私保护计算应用；

c） 组件列表查询接口：用于获取平台内已注册算法组件的概要信息集合；

d） 组件查询接口：用于获取特定算法组件的详细定义、属性列表、输入输出约束等完整信息；
e） 应用列表查询接口：用于获取平台内已注册应用的概要信息集合；
f） 应用查询接口：用于获取特定隐私保护计算应用的编排架构、关联组件详情及部署配置等完整信息。

隐私保护计算的参与方通过数字合约实现隐私保护计算的应用和组件的协商，隐私保护计算公共服务平台可基于数据基础设施实现调用数据基础设施数字合约能力。根据 TC609-6-2025-15《可信数据空间 使用控制技术要求》，在数字合约中，操作行为设置为隐私保护计算，约束条件设置为应用标识符和组件标识符，即各参与方按照应用标识符所指定的应用对合约标的执行隐私保护计算任务，并允许调用应用组件列表中与指定组件标识符制定的组件。

10.3 环境互通

隐私保护计算的多种技术方案有不同的安全能力，抵抗不同强度的内部和外部攻击。数据产品在隐私保护计算公共服务平台和接入连接器交互之前，应对接收端的计算环境进行安全能力的验证。隐私保护公共服务平台之间具有标准化的接口和流程，完成对计算环境安全能力的认证，来保证数据的加工使用能够在符合预期的安全环境下进行。隐私保护计算公共服务平台和接入连接器之间的环境互通，应包含环境验证接口，在任务执行前，调用环境信息采集接口对接收数据的平台/连接器进行安全状态核查，如附录B所示，确保满足数字合约要求。

10.4 计算任务互通

计算任务互通通过标准化接口实现隐私保护计算公共服务平台和接入连接器之间的任务创建、状态同步、执行控制与结果反馈的协同交互。在完成环境与算法验证后，平台将任务配置下发至接入连接器，对方进行任务准入并返回执行状态。执行过程中，各方应支持任务进度、异常事件的实时同步，以及中断恢复和日志对齐，确保跨任务的一致性与可审计性。隐私保护计算公共服务平台和接入连接器之间的隐私保护计算任务互通，应包含以下接口：

a） 创建任务：提交任务配置（输入数据、算法组件、参数、合约 ID 等）；
b） 启动任务：触发任务在受控环境中运行；
c） 查询任务状态：实时获取任务进度、日志、中间结果等；
d） 停止任务：支持异常情况下人工干预终止任务及正常流程下的任务主动终止；
e） 删除任务：清理已完成或失败的任务记录。

11 安全要求

11.1 通用安全

隐私保护计算公共服务平台通用安全符合如下要求：

a） 应符合 GB/T 22239—2019 中规定的第三级以上安全要求；
b） 平台所采用的密码技术应满足国家和行业标准要求；
c） 应具有安全检测与风险评估能力，分析潜在安全风险可能引发的安全事件，提升对网络威胁与攻击行为的识别、分析和主动防御能力；
d） 应具有常见的网络安全事件处置预案，并可针对性进行演练，确保安全事件快速有效处置。

11.2 数据服务安全

11.2.1 数据安全

隐私保护计算公共服务平台需要保证数据安全：

a） 应确保计算过程中数据的保密性、完整性和可用性；
b） 应确保数据和规则只能按照约定的用法、用量进行计算，不能超过数据提供方授权的范围；

c) 应确保数据、中间及最终计算结果不能被参与方、平台的内部人员（如运维人员、研发人员等）非授权获取或滥用；
d) 应保证计算结果的保密性，计算结果是加密处理的，仅数据使用方可解密；
e) 应支持根据数据安全级别调度匹配安全级别的隐私保护计算技术。

11.2.2 过程安全

隐私保护计算公共服务平台数据服务过程符合如下安全要求：
a) 宜支持对公共服务平台的计算环境进行远程验证；
b) 接入连接器应对数据进行加密，应确保只有验证过的计算环境才能对数据进行解密；
c) 数据提供方接入连接器应指定数据使用策略，计算环境应确保严格遵守使用策略。计算环境对使用策略的验证链条应完整，包括数据使用方身份、数据与标识的绑定关系、数据提供方与所持数据的权属绑定关系、授权情况。确保策略不能被伪造、篡改、违背或绕过；
d) 处理多方数据时，应同时满足多个数据提供方的使用策略；
e) 计算环境具备加载动态代码功能时，计算环境应为动态代码提供隔离的运行环境确保动态代码不会危害数据安全；
f) 多个计算环境联合提供服务时，接入连接器应能够验证到所有的计算环境，确保各计算环境的真实性。

11.2.3 传输安全

传输的安全性符合如下要求：
a) 应采用安全的协议保证隐私保护计算各参与方的通信安全；
b) 在通信节点建立连接之前，应进行通信方双向身份认证；
c) 应采用安全的密码技术对通信数据进行保密性和完整性保护，宜使用国产的密码算法和协议；
d) 当通信数据被篡改后，数据接收方应能识别并立即采取措施进行异常处理。

11.3 算法组件安全

算法组件安全符合如下要求：
a) 应支持对算法或模型进行审查，并对审查结果存证，宜支持第三方可信机构对隐私保护计算的算法协议进行评估和测试；
b) 应抵御程序研发人员、运维人员发起的攻击，如篡改程序的预期功能、窥探或导出或留存数据、植入数据访问后门等；
c) 当存在合谋攻击的风险时，应视情形抵御相应阈值的合谋攻击；
d) 应确保参与方无法从获得的结果反推敏感的原始信息；
e) 宜支持纵深防御机制抵抗恶意攻击，如算法能够检测并阻断恶意攻击行为等。

11.4 密钥安全

密钥安全应符合如下要求：
a) 参与方应独立自主地生成用于身份证明的密钥对；宜由权威机构将参与方的身份和公钥进行绑定；
b) 在采用可信执行环境、密态计算等技术时，应用应生成并妥善保管其用于身份证明的密钥对，确保非授权方无法获取私钥；
c) 应支持密钥的安全存储，包括根密钥、派生密钥等。在存储过程中应对密钥及其属性的完整性进行保护；
d) 数据加密密钥只有数据提供方或者其授权的可信应用或者数据提供方授权的数据使用方可以访问，任何非授权主体无法访问数据加密密钥。

11.5 身份安全

身份安全符合如下要求：

a) 应支持对用户、接入连接器、应用分配唯一的标识和身份验证凭证；
b) 应确保身份验证凭证（例如身份密钥、身份证书）的保密性、真实性、可用性和完整性，防止被外部攻击者和参与方窃取或篡改；
c) 应确保标识和标识实体的对应关系不能被篡改；
d) 宜支持对应用进行远程验证，涉及多个可信应用时，可信应用之间也要进行验证。验证通过后颁发身份验证凭证。

11.6 访问控制和权限管理

隐私保护计算公共服务平台访问控制和权限管理安全性符合如下的要求：

a) 在隐私保护计算任务执行过程中，应以最小授权原则为参与方划分权限，各参与方无法获取非本方应获取范围外的信息、进行本方权限外的操作；
b) 数据在被使用之前应进行鉴权，确保授权主体的真实性，授权内容的完整性，防范篡改、伪造等数据安全风险；
c) 进行全过程的校验，包括在数据及数据使用后的结果发送给数据使用方前，对数据使用方身份、数据与标识的绑定关系、数据提供方与所持数据的权属绑定关系、数据使用策略等进行检验；
d) 应具备针对参与方和数据用途的授权机制，仅当数据提供方明确授权后，数据才能参与隐私保护计算任务；
e) 宜具备完整的角色和权限体系，参与方登录后要有明确的角色，并匹配约定的权限。

11.7 计算环境安全

计算环境为计算过程提供保护，满足如下要求：

a) 宜具备可信根，接入连接器可以通过可信根用于验证系统从启动到运行的各个环节的安全性确认环境启动过程的安全性；
b) 可信根宜由权威机构背书，即根据可信根的身份标识可在该权威机构获取用于验证其身份的公钥；
c) 应确保环境内的运行状态不会被窥探或篡改，能够抵御来自环境外的攻击；
d) 输出到环境外部的数据，应进行加密等防护措施，保证数据在环境外的安全存储；
e) 应提供相应的机制，确保只有通过了完整性验证的程序才能在环境中运行，防止恶意程序的运行。

11.8 安全审计

安全审计是在隐私保护计算任务完成后的安全控制手段，符合如下的要求：

a) 应具备对接入隐私保护计算系统内的用户的操作行为、任务的执行状态、计算过程、数据的访问记录、数据的使用历史等进行存证的能力；
b) 应在隐私保护计算任务执行的各环节中，对各个参与方的数据使用操作进行存证；
c) 应对用于隐私保护计算任务的运行代码进行存证，包含算法镜像、配置模板及关键参数等；
d) 应支持对存证结果进行查询和审计，审计内容宜包括访问其它参与方的数据、非授权行为、出域的数据传输等；
e) 发生安全事件时，应支持对安全事件的跟踪和追溯；
f) 应支持存证记录的完整性、保证存证信息的真实性。宜采用可信计算、区块链等技术保证存证完整性。

附 录 A
（资料性）
隐私保护计算平台的服务示例

A.1 基于推理服务的视频生成

在数字内容创作日益普及的背景下，用户希望将一组静态照片（如家庭聚会、团队合影、旅行留影等）自动合成为一段具有动态效果的视频（如人物微笑增强、动作补间、背景音乐匹配、场景过渡融合），实现“老照片动起来”的智能体验。这一过程涉及两类敏感数据：一是用户上传的照片，可能包含人脸、身份和时空信息等个人敏感信息；二是用于生成视频的预训练或定制化大模型，属于企业的核心商业资产。

隐私保护计算公共服务平台为大模型推理提供可信执行环境，保障模型代码与用户输入数据在计算过程中的保密性与完整性。在可信执行环境内完成图像特征提取、动作补间、场景融合与配乐匹配等推理任务，生成的视频文件经加密后安全输出至用户。原始照片及提取的人脸特征全程处于受控环境，不被留存、访问或泄露。

A.2 基于数据分析服务的广告转化效果统计

在跨平台数字营销场景中，广告主希望评估其在流媒体平台投放的广告是否有效提升了在第三方电商平台的实际销量。依托隐私保护计算公共服务平台，广告主可编写用于衡量转化效果的 SQL 查询逻辑，并将该逻辑部署到可信执行环境，安全执行转化率计算，确保数据在分析过程中不被泄露或滥用。这一过程中涉及三类敏感数据：一是广告平台侧的用户曝光与观看记录，二是电商平台侧的用户购买行为数据，三是用于 SQL 逻辑测试的历史观看与购买数据。

隐私保护计算公共服务平台应提供完整的 SQL 开发与调试环境，支持数据使用方编写、测试和优化用于隐私保护计算的查询逻辑。平台需支持开发标准化的 SQL 查询语句，并确保其可在可信执行环境（TEE）中安全部署与执行。在正式运行阶段，平台为内执行 SQL 查询语句的执行提供安全的环境，确保用户提供的观看记录、购买行为的真实数据不会被留存、访问或泄露。

A.3 基于推理服务的跨机构联合风控

银行在开展信贷审批业务时，希望借助第三方数据平台（如电商、运营商）的用户行为数据提升风险识别能力。该场景涉及多方敏感数据协作：银行掌握用户的金融资质信息（如收入、负债），第三方平台则拥有用户的消费习惯、通信行为等多维特征。

隐私保护计算公共服务平台提供隐私集合求交（PSI）对数据集的标识列进行分析，在不泄露非交集用户信息的前提下，安全匹配双方共同用户，形成对齐样本。基于此，平台支持在联邦学习框架下（如 XGB、SS-LR 等算法）开展联合建模，各方在本地训练模型并仅交换加密梯度，实现模型协同优化，提升风控模型的准确性与泛化能力。对于新用户，平台进一步支持联合推理，利用已训练模型在保护各方输入数据保密性的前提下输出风险评分。

A.4 基于隐匿查询的智能来电识别

在移动通信场景中，用户接到陌生电话时，希望实时判断该号码是否为骚扰、诈骗或营销电话，以提升通信安全。为此，客户端需向拥有大规模标记数据库的服务商查询号码标签信息。然而，用户不希望服务商获知其实际查询的号码，以防止个人通信隐私泄露；同时，服务商也希望保护其数据库内容不被推断或探测。

隐私保护计算公共服务平台提供基于隐匿查询服务。客户端在本地对目标号码进行加密处理，构造隐私保护查询请求，服务端在无法获知具体查询号码的前提下，根据请求在其骚扰电话数据库中定位并返回对应的标签信息（如“骚扰”“诈骗”“安全”等）。整个过程确保用户查询内容的保密性，服务端仅执行受限访问，无法推断用户行为。平台保障查询操作的安全协议执行，实现“查得到、看不见”的隐私保护来电识别服务。

附 录 B
（规范性）
隐私保护计算公共服务平台和接入连接器交互接口

B.1 概述

隐私保护计算公共服务平台和接入连接器之间的接口列表如B.1所示。

表 B.1 接口列表

序号	接口名称	接口编码	调用方	提供方
1	环境信息采集接口	/environmentInformationCollection	接入连接器	隐私保护计算公共服务平台、接入连接器
2	组件注册接口	/componentRegistration	接入连接器	隐私保护计算公共服务平台
3	应用注册接口	/applicationRegistration	接入连接器	隐私保护计算公共服务平台
4	组件列表查询接口	/componentListQuery	接入连接器	隐私保护计算公共服务平台
5	组件查询接口	/componentQuery	接入连接器	隐私保护计算公共服务平台
6	应用列表查询接口	/applicationListQuery	接入连接器	隐私保护计算公共服务平台
7	应用查询接口	/applicationQuery	接入连接器	隐私保护计算公共服务平台
8	创建任务接口	/createTask	隐私保护计算公共服务平台	接入连接器
9	启动任务接口	/startTask	隐私保护计算公共服务平台	接入连接器
10	查询任务接口	/queryTask	隐私保护计算公共服务平台、接入连接器	隐私保护计算公共服务平台、接入连接器
11	停止任务接口	/stopTask	隐私保护计算公共服务平台、接入连接器	隐私保护计算公共服务平台、接入连接器
12	删除任务接口	/deleteTask	隐私保护计算公共服务平台	接入连接器

B.2 环境信息采集接口

环境信息采集接口符合B.2的要求。

表 B.2 环境信息采集接口

接口名称	环境信息采集接口				EnvironmentInformationCollection	
接口访问地址	/environmentInformationCollection				HTTP Method	POST
功能	数据提供方收集隐私保护计算公共服务平台或数据接收方的环境信息，用于后续验证环境是否符合预期					
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	请求编号	request_id	string	—	必选	请求唯一标识
2	时间戳	timestamp	int64	—	必选	请求时间戳（毫秒）
3	环境	environment_id	string	—	可选	指定环境 ID（空则查询当前）

	编号					
4	包含的数据段	include_sections	array<string>	—	必选	明确收集指定环境的哪些字段的信息，”capabilities”,”properties”,”evidence”
5	是否采集证据	collect_evidence	bool	—	可选	是否在本次请求中触发远程证明证据采集，默认为 false
6	证据类型	evidence_types	array<string>		可选	当 collect_evidence=true 时有效，指定需采集的证据类型，如：["tdx_quote","event_log", "platform_config"]。若未指定，默认返回平台支持的全部证据类型。
7	是否包含签名	include_signatures	bool	—	必选	指示返回的证据是否需包含数字签名，用于验证真实性
8	过滤条件	filter_conditions	array<string>	—	可选	用于对返回的环境属性或能力进行过滤的条件表达式列表
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	时间戳	timestamp	int64	—	必选	请求时间戳（毫秒）
3	数据采集时间	collection_time	int64	—	必选	采集证据的时间
4	能力声明列表	capabilities	array<Object>	—	条件	描述能支持的能力，如加密算法、隔离级别等。仅在成功且需要时返回
5	环境属性	properties	map<String,Any>	—	条件	描述运行环境的元信息，如 OS 版本、内核参数、容器 ID 等。仅在成功时可选返回
6	证据包	evidence_bundle	object	—	条件	包含原始证明材料（如 quote、event log 等），仅在 collect_evidence=true 时返回
7	证据元数据	evidence_metadata	object	—	条件	描述证据的格式、类型、签名算法等元信息，用于验证方解析证据

B.3 组件注册接口

组件注册接口符合B.3的要求。

表 B.3 组件注册接口

接口名称		组件注册接口			ComponentRegistration	
接口访问地址		/componentRegistration			HTTP Method	POST
功能		参与方接入连接器向隐私保护计算公共服务平台注册隐私保护计算组件				
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	标识码	connectorId	string	—	必选	接入连接器唯一标识
2	组件域	domain	string	—	必选	不同厂家是不同域名，比如厂家A，厂家B 不同的算法类型，比如预处理类的，计算类、建模类
3	组件名称	name	string	—	必选	组件名称

4	组件描述	description	string	—	必选	对组件功能、用途等的详细说明
5	组件版本	version	string	—	必选	组件版本
6	属性值列表	attribute	repeated struct	—	必选	组件运行所需的参数，如： PSI 组件需要指定 PSI 协议（RR22\ECDH\KKRT）、求交列、结果接收方等
6.1	属性名称	attr.name	string		必选	属性名称
6.2	属性类型	attr.type	string		必选	属性类型枚举，如AT_STRING、AT_FLOAT、

6.3	属性的约束	attr.atomic	JSON		必选	描述属性的默认值、上边界、下边界等，如：
						"atomic": {
						isOptional": true,
						"allowedValues":
						{
						"ss": [
						"==",
						"<",
						"<=",
						">",
						">=",
						"IN",
						"NOTNULL"
						]
						}
						}

7	输入数据列表	inputs	repeated struct	—	必选	输入数据列表，要和组件定义或申明保持一致
7.1	参数名称	input.name	string		必选	输入参数的名称
7.2	参数描述	input.desc	string		可选	输入参数的详细描述
7.3	参数类型	input.type	string		可选	输入的类型,如： 表格,table.individual 报告,report 模型,model.ss_glm
8	输出数据列表	output	repeated struct	—	必选	输出数据列表，顺序要和组件定义或申明保持一致
8.1	参数名称	output.name	string		必选	输出参数的名称
8.2	参数描述	output.desc	string		可选	输出参数的描述
8.3	参数类型	output.type	string		可选	输入的类型如： 表格,table.individual 报告,report 模型,model.ss_glm
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	组件标识码	componentId	string	XX	必选	返回组件标识码

B.4 应用注册接口

应用注册接口符合B.4的要求。

表 B.4　应用注册接口

接口名称		应用注册接口		ApplicationRegistration		
接口访问地址		/applicationRegistration		HTTP Method		POST
功能		参与方接入连接器向隐私保护计算公共服务平台注册隐私保护计算应用				
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	标识码	connectorId	string	—	必选	接入连接器唯一标识
2	应用名称	name	string	—	必选	应用名称
3	应用描述	description	string	—	必选	对应用功能、用途等的详细说明
4	应用版本	version	string	—	必选	应用版本
5	组件列表	components	repeated string	—	必选	应用支持的组件列表
6	容器列表	containers	repeated container	—	必选	应用将以容器的方式被运行起来。该字段描述应用被拉起的容器信息
6.1	容器名称	container.name	string	—	可选	容器名称
6.2	镜像信息	container.image	string	—	必选	容器镜像
6.3	启动命令	container.command	string	—	可选	程序启动命令
6.4	启动参数	container.args	string	—	可选	启动命令参数
6.5	工作目录	container.working_dir	string	—	可选	容器工作目录
6.6	通信端口列表	container.port	struct	—	可选	运行底座会按照该字段的描述为应用配置跨参与方通信的端口
6.6.1	端口名称	port.name	string		可选	端口名称
6.6.2	端口协议	port.protocol	string		可选	枚举，如gRPC、HTTP
6.6.3	端口开放范围	port.scope	string		可选	枚举，如 Cluster:集群内开放 Party:参与方开放 Local:本地/容器内开放
6.6.4	端口号	port.port	string		可选	端口编号，取值1-65535
7	配置模板	configTemplate	map<string,string>		可选	应用运行所需的配置文件的模版，模版中的占位符会在应用被启动前由运行底座渲染成真正的取值
响应参数：						

1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	组件标识码	applicationId	string	XX	必选	返回应用标识码

B.5 组件列表查询接口

组件列表查询接口符合B.5的要求。

表 B.5 组件列表查询接口

接口名称		组件列表查询接口				ComponentListQuery
接口访问地址		/componentListQuery				HTTP Method POST
功能		接入连接器向隐私保护计算公共服务平台提交组件列表查询请求，查询平台上注册的组件列表				
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务节点唯一标识
2	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	组件列表信息	componentList	JSON	—	必选	返回组件列表，包含每个组件的一下信息：componentId,domain，name,description，version

B.6 组件查询接口

组件查询接口符合B.6的要求。

表 B.6 组件查询接口

接口名称		组件查询接口				ComponentQuery
接口访问地址		/componentQuery				HTTP Method POST
功能		接入连接器向隐私保护计算公共服务平台查询某个组件的具体信息				
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，连接器发起为接入连接器唯一标识，业

						务节点发起为业务节点唯一标识
2	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败
2	组件信息	componentInfo	JSON	—	必选	返回组件的信息，包含每个组件一下信息：componentId,domain,name,description,version,attribute,inputs,outputs

B.7 应用列表查询接口

应用列表查询接口符合B.7的要求。

表 B.7 应用列表查询接口

接口名称		应用列表查询接口			ApplicationListQuery	
接口访问地址		/applicationListQuery			HTTP Method	POST
功能		接入连接器向隐私保护计算公共服务平台提交查询请求，查询平台上注册的应用列表信息				
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务节点唯一标识
2	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败
2	应用列表信息	applicationList	Json	—	必选	返回应用列表信息，其中应用包含以下信息：applicationId,name,version

B.8 应用查询接口

应用查询接口符合B.8的要求。

表 B.8 应用查询接口

接口名称		应用查询接口			ApplicationQuery	
接口访问地址		/applicationQuery			HTTP Method	POST
功能		接入连接器向隐私保护计算公共服务平台提交查询请求，查询平台上某个具体应用的信息				
请求参数：						
序	参数名	字段名称	数据类型	长	可选	说明

号	称			度	/ 必选	
1	应用标识码	applicationId	string	2	必选	组件的唯一标识码
2	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务节点唯一标识
3	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	应用信息	applicationInfo	JSON	—	必选	返回组件的信息，包含：name,version,description, components,containers,configTemplate

B.9 创建任务接口

创建任务接口符合B.9的要求。

表 B.9 创建任务接口

接口名称	创建任务接口				CreateTask	
接口访问地址	/createTask				HTTP Method	POST
功能	隐私保护计算公共服务平台向接入连接器下发新任务的配置信息					
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	任务唯一编码	taskId	string	—	必选	任务的唯一标识码
2	应用名称	appName	string	—	必选	Application的名称
3	组件运行所需的实参	parameters	Map<string,string>	—	必选	组件运行所需的实参
4	任务参与方	parties	Repeat string	—	必选	任务的参与方
5	任务运行所需资源	resource	JSON	—	可选	任务执行预计所需的资源 CPU、Memery
6	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务节点唯一标识
7	发起用	issuerEntityId	string	—	必选	发起方用户主体身份标

	户主体标识码					识码
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。

B.10 启动任务接口

启动任务接口符合B.10的要求。

表 B.10 启动任务接口

接口名称		启动任务接口				StartTask	
接口访问地址		/startTask				HTTP Method	POST
功能		隐私保护计算公共服务平台向接入连接器下发启动任务的指令					
请求参数：							
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明	
1	任务唯一编码	taskId	string	2	必选	任务的名称	
2	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务节点唯一标识	
3	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码	
响应参数：							
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。	

B.11 查询任务状态接口

查询任务接口符合B.11的要求。

表 B.11 查询任务接口

接口名称		查询任务接口				QueryTask	
接口访问地址		/queryTask				HTTP Method	POST
功能		隐私保护计算公共服务平台或接入连接器提供任务状态的查询接口					
请求参数：							
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明	
1	任务唯一	taskId	string	2	必选	任务唯一标识	

	编码					
2	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务节点唯一标识
3	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	返回任务状态码	taskStatusCode	string	2	必选	返回任务的状态： 0：未指定的状态（默认值，通常表示无效或未初始化 1: 表示任务处于等待中，即任务已提交但尚未开始执行 2：表示运行中，任务已启动并执行 3：成功完成 4：失败 5:停止中，已收到停止请求，系统正在终止任务，但尚未完成

B.12 停止任务接口

停止任务接口符合B.12的要求。

表 B.12 停止任务接口

接口名称	停止任务接口				StopTask	
接口访问地址	/stopTask				HTTP Method	POST
功能	隐私保护计算公共服务平台或接入连接器提供停止任务的接口					
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	任务唯一编码	taskId	string	2	必选	任务唯一标识
2	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务

						节点唯一标识
3	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码
响应参数：						
1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	返回任务状态码	taskStatusCode	string	2	必选	返回任务的状态： 0：未指定的状态（默认值，通常表示无效或未初始化 1：表示任务处于等待中，即任务已提交但尚未开始执行 2：表示运行中，任务已启动并执行 3：成功完成 4：失败 5：停止中，已收到停止请求，系统正在终止任务，但尚未完成

B.13 删除任务接口

删除任务接口符合B.13的要求。

表 B.13 删除任务接口

接口名称	删除任务接口				DeleteTask	
接口访问地址	/deleteTask				HTTP Method	POST
功能	隐私保护计算公共服务平台或接入连接器提供停止任务的接口					
请求参数：						
序号	参数名称	字段名称	数据类型	长度	可选/必选	说明
1	任务唯一编码	taskId	string	2	必选	任务唯一标识
2	发起主体标识码	issuerId	string	—	必选	发起主体唯一标识，接入连接器发起为接入连接器唯一标识，业务节点发起为业务节点唯一标识
3	发起用户主体标识码	issuerEntityId	string	—	必选	发起方用户主体身份标识码
响应参数：						

1	执行结果状态	status	string	2	必选	执行结果状态： 0:成功；1:失败。
2	返回任务状态码	taskStatusCode	string	2	必选	返回任务的状态： 0：未指定的状态（默认值，通常表示无效或未初始化 1: 表示任务处于等待中，即任务已提交但尚未开始执行 2：表示运行中，任务已启动并执行 3：成功完成 4：失败 5:停止中，已收到停止请求，系统正在终止任务，但尚未完成

参 考 文 献

[1] GB/T XXXXX-XXXX 数据基础设施 参考架构
[2] GB/T XXXXX-XXXX 数据基础设施 互联互通基本要求
[3] GB/T XXXXX-XXXX 数据基础设施 用户身份管理和接入规范
[4] GB/T XXXXX-XXXX 数据基础设施 标识要求
[5] GB/T XXXXX-XXXX 数据基础设施 连接器技术要求
[6] GB/T XXXXX-XXXX 数据基础设施 数据目录描述要求
[7] TC609-6-2025-13 数据基础设施 安全能力通用要求
[8] TC609-6-2025-01 可信数据空间 技术架构
[9] TC609-6-2025-14 可信数据空间 数字合约技术要求
[10] TC609-6-2025-15 可信数据空间 使用控制技术要求
[11]YD/T 4947-2024 隐私计算 可信执行环境产品安全要求
[12]YD/T 4948-2024 隐私计算 可信执行环境产品性能测试要求
[13]YD/T 4690-2024 隐私计算 多方安全计算产品安全要求和测试方法
[14]YD/T 4691-2024 隐私计算 联邦学习产品安全要求和测试方法
[15]YD/T 4692-2024 隐私计算 联邦学习产品性能要求和测试方法
[16]ISO/IEC 18033-6:2019 信息技术 加密算法 第 6 部分：同态加密