ICS 35.240.99
CCS L67

T/CCIASC

中 国 计 算 机 行 业 协 会 团 体 标 准

T/CCIASC 0023—2024

多方安全计算互联互通技术规范

Technical Specification for Interoperable Multi-Party Secure Computation

2024－12－06 发布　　2024－12－12 实施

中国计算机行业协会　　发 布

目　　次

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。

本文件由成都卫士通信息安全技术有限公司提出。

本文件由中国计算机行业协会归口。

本文件起草单位：成都卫士通信息安全技术有限公司、上海富数科技有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、北京瑞莱智慧科技有限公司、清华大学、中车信息技术有限公司、中铁建设集团有限公司、中铁建网络信息科技有限公司。

本文件主要起草人：齐伟钢、刘从祥、陈建林、郭潇、包佳奇、李静、陆文金、张舒黎、曹占涛、雷术梅、张小青、陈华楠、吴梦丹、周瑞、彭夕茊、李夷苒、望娅露、张兆雷、张玉峰、杨天雅、李斌、李其然、韩毅斌、张振威、吴碧莹、康伟德、姜佳岐、王安宇、马世和、唐刚、张德馨、李尤、安健、杜岚、高闻远。

引　言

随着多方安全计算技术的发展，越来越多的技术服务厂商研发了自己的多方安全计算平台，或服务于自有生态，或服务于金融机构，或服务于政府机构，将原本独立存在的数据孤岛连接了起来，实现了“数据的可用而不可见”。另一方面，因不同的多方安全计算平台大多基于自有知识产权的算法原理和系统设计实现，并且闭源的平台居多，平台之间原生无法完成信息的交互，将“数据孤岛”变成了“计算孤岛”，因此发布多方安全计算互联互通技术规范非常有必要。

本文件提出了多方安全计算跨平台互联互通标准框架，并通过在节点互联、数据资源互联、算法组件互联中对概念定义、管理、认证、存证、互联操作、通信等方面提出了明确要求，并且提供了明确的互联互通接口，确保符合本协议的多方安全计算平台能够相互发现、建立连接，为节点互通、资源互通、算法互通提供基础环境。

多方安全计算互联互通技术规范的发布，将加快形成统一标准体系、促进互联互通新生态构建、助力数据流通体系监管落地，进而推动数据要素市场的规范化发展。

多方安全计算互联互通技术规范

1 范围

本文件提出了多方安全计算跨平台互联互通标准框架，并通过在节点互联、数据资源互联、算法组件互联中对概念定义、管理、认证、存证、互联操作、通信等方面提出了明确的要求，并提供了具体的互联互通接口，确保符合本规范的多方安全计算平台能够相互发现、建立连接，为节点互通、资源互通、算法互通提供基础环境，从而实现异构平台的互联互通。

本文件适用于指导多方安全计算平台跨平台互联互通任务协同的研发、测试和验收等工作。

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。

BDC 63-2021 多方安全计算跨平台互联互通 第一部分：总体框架

GB/T 25069-2022 信息安全技术 术语

3 术语和定义

BDC 63-2021界定的以及下列术语和定义适用于本文件。

3.1

多方安全计算平台 secure multi-party computation

指基于密码学协议和技术实现的、用于进行多个参与者数据计算的完整系统，旨在允许多个参与者在不暴露各自原始数据的完成数据的计算和统计，其核心目标是确保参与者能够共享信息进行计算，同时保持他们的原始数据的保密性。

3.2

互联互通 interoperability

互联互通是指具有不同系统架构或功能实现方案的多方安全计算平台之间通过统一规范的接口、协议等实现跨平台的数据、算法、计算任务的交互与协同，以支持部署不同平台产品的用户共同完成同一计算任务。

3.3

数据集 dataset

隐私计算中某一参与方参与计算的一条或多条数据的集合。数据集以不同形式存储，常见的存储解决方案包括 MySQL、HIVE、文件（CSV、TXT）等。

3.4

任务 job

任务是指基于各合作方数据进行的一次具体的计算过程。多方安全计算平台接收各数据方的加密数据后，按照协定的算法执行，并将计算结果发送给结果接收方。

3.5

模型 model

本文件中主要指机器学习模型，指对数据的某种数学表达式或算法，其目的是根据输入的数据进行学习，然后对新数据进行预测或决策，主要通过学习数据中的模式、关系和规律来实现其功能。

3.6

组件 component

用于执行隐私计算任务的一种可代替、可组合、可独立部署的部件，封装了某个特定计算或算法

的模块单元的实现并提供一系列可用的接口，被使用在隐私计算流程 DAG 中，用顶点（vertex）表示。

3.7

流程 flow

采用 DAG 结构定义的、可编排的算法组件流，可对流程进行启动、停止、暂停等操作。

3.8

项目 project

项目是指在多方安全计算环境中，为实现特定目标（如数据分析、机器学习模型训练、数据共享等）而定义的一个完整的工作流程。这个工作流程通常包括数据源、数据处理方法、流程、计算任务、以及最终的结果输出等。

3.9

东西向接口 east-west interface

东西向接口指不同多方安全计算平台间同一层级或模块、组件之间的交互接口。它主要用于支持不同参与方之间的数据和计算的直接交换。

3.10

南北向接口 north-south interface

南北向接口指同一多方安全计算平台内部之间的交互接口，主要用于支持不同层级（如应用层和服务层）之间的数据和计算的交互。

4 符号和缩略语

下列符合和缩略语适用于本文件。

DAG	Directed Acyclic Graph	有向无环图
RPC	Remote Procedure Call	远程过程调用
FL	Federated Learning	联邦学习
MPC	Secure Multi-Party Computation	多方安全计算
PIR	Private Information Retrieval	隐私信息检索
SSL	Secure Sockets Layer	安全套接字协议
TLS	Transport Layer Security	传输层安全协议

5 概述

5.1 相关概念

5.1.1 节点

多方安全计算节点是互联互通网络的基本组成单元，对外提供交互接口。每个多方安全计算节点都可以创建多方安全计算项目，也可以加入其他节点的多方安全计算项目。

多方安全计算互联互通首先要实现节点的互联，应保证异构节点之间可以相互发现、相互建立连接、相互授权、相互同步状态等。

节点的内部对象模型如下图所示：

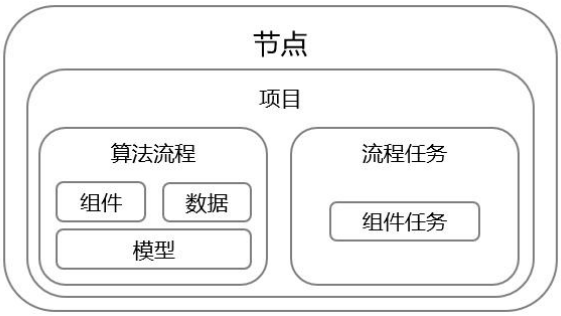

图 1 多方安全计算节点示意图

5.1.2 资源

在多方安全计算系统中，资源通常指参与计算的各个实体，主要包含节点资源、项目资源、数据资源、组件资源、模型资源等类别。

表 1 资源类型

序号	资源类别	代码	类型前缀
1	节点资源	Node	N
2	项目资源	Project	P
3	数据资源	Dataset	D
4	组件资源	Component	W
5	模型资源	Model	M

每一类资源都有自己的 ID。其中节点资源 ID 在全网唯一，项目资源、数据资源、组件资源、模型资源的 ID 在节点范围内唯一。不同节点资源间可以在密文状态下交互项目资源、数据资源、组件资源及模型资源；在节点内部，数据资源经过组件资源的处理及计算可产生模型资源，如下图所示。

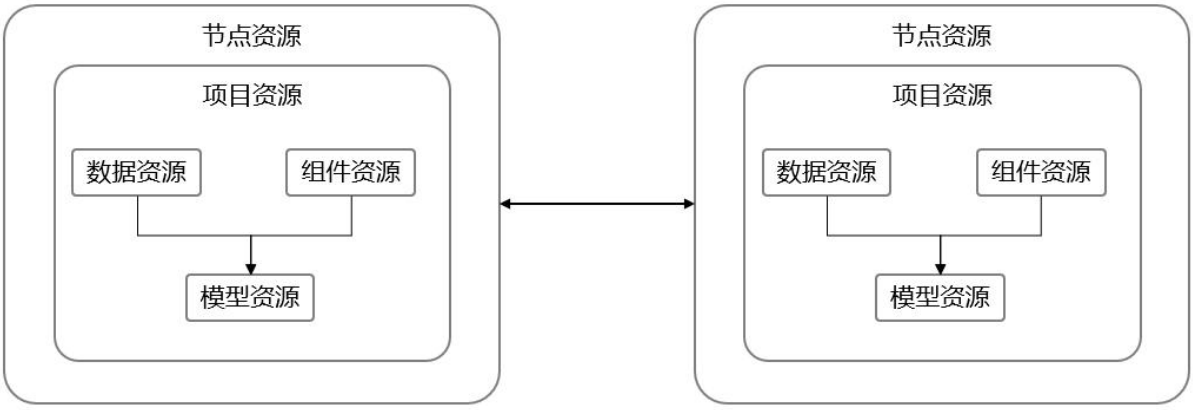

图 2 资源相关概念关系示意图

5.1.3 算法组件

算法组件是在特定容器内可独立运行的软件单元，在多方安全计算环境里，是一个内聚了对数据处理功能的逻辑单元，包含输入数据、输出数据、统计数据、计算规则、计算结果等，并提供了一系列可用的接口。

在多方安全计算互联互通过程中，算法组件互联应考虑算法组件、组件任务、算法流程、流程任务层面的互联，关系如图：

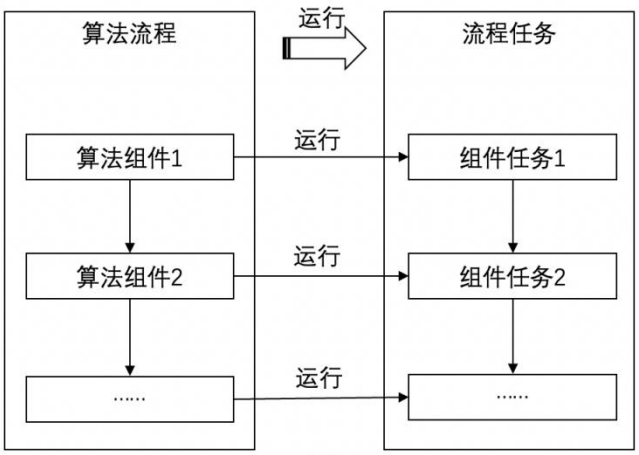

图 3 算法组件相关概念关系示意图

5.1.4 通信协议

通信协议是多方安全计算互联互通中的一组约定和标准，旨在指导参与方在进行数据交换和协同计算时，如何安全、有效地传输信息，确保数据在多个计算参与者之间的传递和处理符合隐私保护原则，并能有效支持隐私计算的相关操作。主要包含通信接口、通信框架、数据格式、加密机制和网络环境等。

5.2 互联互通原则

多方安全计算互联互通应遵循如下原则：

a) 互通性，不同多方安全计算平台间应支持通用、规范的通信接口和互联协议，能够进行跨平台的通信、数据交换、互联操作和状态同步；
b) 平台自治性，各技术平台均应为自治系统，独立管理平台内部的任务协同与资源配置，参与多方安全计算互联互通任务时，各平台无需暴露内部的私有协议、模块设置和架构细节；
c) 安全性，不同技术平台间的交互和协同应通过统一的安全通信机制、认证与授权机制、安全模型假设等保障多方安全计算互联互通的通信安全、应用安全、算法协议安全；
d) 正确性，多方安全计算互联互通完成的多方安全计算任务与各平台独立完成的多方安全计算任务结果保持一致，或偏差在不影响应用的范围内；
e) 易扩展性，多方安全计算互联互通应在组网能力、技术迭代、功能升级等方面具备扩展性，应支持通信协议的扩展升级，应支持新定义类型的节点接入，应支持新算法组件的添加和迭代，应支持节点间互联互通新功能的扩展升级；
f) 兼容性，多方安全计算互联互通应在操作系统、运行环境、第三方库、数据存储系统、算法组件等方面具备兼容性；
g) 开放性，不同多方安全计算平台间应协商设计统一开放的对外接口，同时支持二次开发。

5.3 互联互通要求

图 4 多方安全计算互联互通要求概览图

如图 4 所示，多方安全计算互联互通要求主要包含：

a) 节点互联要求，主要包含节点定义、节点认证要求、节点存证要求、节点管理、互联操作、互通接口、节点同步等；
b) 资源互联要求，主要包括资源定义、资源认证要求、资源存证要求、资源管理、互联操作、互通接口、资源同步等；
c) 算法组件互联要求，主要包括数据输入输出规范、算法流程编排规范、组件认证要求、组件存证要求、组件流程管理、互联操作、互通接口、任务同步等；
d) 通信协议互联要求，多方安全计算互联互通以统一的平台间通信要求为基础，通过参与方协商在通信接口、通信框架、数据格式、加密传输机制、网络环境等方面达成共识。

6 节点互联要求

6.1 节点定义

节点信息应包含的信息项如下：

a) 节点 ID：全网唯一、不可篡改的节点 ID；
b) 节点名称；
c) 所属组织；
d) 数字证书；
e) 对外协同服务地址：协同服务地址，包含域名、IP、端口、协议等，提供查询及协同服务接口，正式生产环境必须通过拥有数字证书的 https 提供服务；
f) 对外多方安全计算服务地址：多方安全计算服务地址，包含域名、IP、端口、协议等，仅用于多方安全计算任务的执行，正式生产环境必须通过拥有数字证书的 https 提供服务；
g) 对内管理运营服务地址：内部管理运营的服务地址。不对外公开 ；
h) 对内组件服务地址：内部组件服务地址。不对外公开；

i） 扩展信息：包含节点描述、节点功能信息、节点物理位置、节点维护人员信息、资源概况描述、节点可承担的多方安全计算参与方角色类型、节点支持的多方安全计算技术类型和加密协议等。

6.2 节点认证要求

节点加入多方安全计算互联互通网络前应经过双向身份认证，确保连接节点身份可信，具体要求包括：

a） 节点身份认证应符合国家、行业标准和要求，宜支持国密算法；
b） 节点身份认证宜采用两种或两种以上组合的认证方式实现；
c） 节点认证应满足以下原则：
1） 唯一性，节点认证的标识应具备全局唯一性和不可更改性；
2） 可信性，节点身份应通过可信第三方认证或通过分布式共识机制保障可信性；
3） 可认证性，应具有安全身份认证机制；
4） 可维护性，应支持节点身份全生命周期维护和管理。

6.3 节点存证要求

节点存证指节点在多方安全计算互联互通任务中应具备对关键数据和关键行为进行记录的能力，以满足后续内外部监管审计以及任务责任归属追溯的需要。存证内容包括以下：

a） 应支持对节点信息存证，确保该节点后续可被辨识，其中数字证书可被认证；
b） 应支持对节点涉及的流入流出资源的摘要存证，同时记录该节点对资源的用法、用量的行为日志；
c） 应支持对节点在计算任务执行过程中的重要环节日志存证，例如：节点连接/断开、算法组件加载、资源流入、资源流出、任务启动、任务结束、执行结果、异常信息等；
d） 应支持对节点与其他节点达成合作关系的协议存证，以及各方协商达成的一系列互联互通协作共识和约定。

6.4 节点管理

节点管理指节点内部用于维持节点正常运作的基本能力，应包含：

a） 应支持节点的管理，包括：节点注册、注销、变更、配置等；
b） 应支持节点信息的维护，包括：节点信息增加、删除、修改、查询等；
c） 应支持角色组和角色管理，包括：新增角色组、新增角色，编辑角色组、编辑角色，删除角色组、删除角色，角色授权。角色设置应最小覆盖参与多方安全计算互联互通任务的所有参与方主体，包括发起方、数据方、算法方、计算方、结果方、协调方等；
d） 应支持节点权限管理，包括：资源访问权限，指对本地或外部资源的打开、可读、编辑、拷贝等权限；资源控制权限是指对本地资源的使用、禁用，可视、屏蔽的控制权限；动作权限，指对平台窗口中的可视对象进行菜单项、按钮、下拉列表框、数据编辑、记录增加、记录删除等动作权限；操作权限，指通过认证授权后参与多方安全计算任务，并与其他节点协同完成计算过程中涉及到的一系列操作操作权限。

6.5 节点互联操作

节点之间应在相互通过身份认证、获得访问授权、保证通信安全的条件下，建立互联关系，以相互提供节点服务的形式进行合作。

6.5.1 节点发布

节点注册成功后，应向平台提交节点发布请求，然后节点的部分公开信息出现在节点列表上，可供其他节点检索和查询。

6.5.2 节点发现

节点应检索并查看其他节点发布的节点信息，如有合作意愿后续可发起项目邀请。

6.5.3 节点授权

节点应通过授权签约来确定合作关系，合作节点确认签约后才正式建立连接关系。节点合作关系的建立是资源互联和算法组件互联的基础，没有签约成功的资源互联或组件互联都会被拒绝。

6.6 互通接口

节点互通应包含如下接口，具体接口规范参见附录A：

a) 东西向接口，应包含节点信息查询、合作申请发起、更新合作意向、节点合约解除、更新节点信息、节点合作查询、节点健康探测等；
b) 南北向接口，应包含节点信息查询、节点信息更新等。

6.7 节点同步

节点应具备将自身服务状态同步至其它合作方的能力。

7 资源互联要求

7.1 资源定义

多方安全计算平台中主要包含节点资源、数据资源、项目资源、组件资源、模型资源等，相关资源信息应包含的信息项有：

a) 节点资源的基本信息包括：唯一的节点资源 ID、资源名称、资源地址、所属组织等。可选的，节点资源的扩展信息包括：服务状态等；
b) 数据资源基本信息包括：唯一的 ID、名称、位置（地址）、所属组织、所属节点、数据字典、版本号、状态（在线/下线/离线）。可选的，数据资源的扩展信息包括：样例数据、用法（支持的算法组件）、用途（受限的使用范围）、用量（受限的使用数量）、资源大小（行数、维度数、文件大小等）、其他特性（稀疏性、样本平衡）；
c) 项目资源的基本信息包括：唯一的 ID、名称、类型、组件版本、所属组织（开发者）、状态、创建时间。可选的，项目资源的扩展信息包括：描述信息、修改时间等；
d) 组件资源的基本信息包括：唯一的 ID、名称、位置（地址）、所属组织（开发者）、所属节点、版本号、发布日期、安全认证信息、签名、版权信息、提供方式（组件包|服务）、状态（在线/下线/离线）。可选的，组件资源的扩展信息包括：运行环境信息、组件包大小、输入与输出信息、兼容性信息、帮助信息 ；
e) 模型资源的基本信息包括：唯一的 ID、名称、位置（地址）、所属组织（开发者）、所属节点、版本号、发布日期、版权信息、提供方式（离线模型|在线模型）、状态（在线/下线/离线）。可选的，模型资源的扩展信息包括：使用样例、用途、输入与输出信息、帮助信息。

7.2 资源认证要求

多方安全计算互联互通中，各节点提供的资源需要遵循统一认证机制，能够证明各自数据与模型等资源的所有权，确保不同节点资源在互联互通过程中安全可信。

资源认证可通过数字签名形式实现，数据拥有者在发布数据资源的同时，公布资源文件所对应的公钥及相应的数字签名。对于多文件资源，协议需定义相应的签名算法。

发布在多方安全计算互联互通网络中的资源宜通过权威机构认证，资源包括发布的各类数据资源、算法组件资源、模型资源等。数据资源的认证宜基于数据提供方角色进行认证，确保数据提供方的可信性、合法性、可追溯性等。

7.3 资源存证要求

资源存证指平台应对多方安全计算互联互通任务中的数据资源、算法资源、模型资源使用情况和关键资源摘要进行记录，以保证备份记录在一定期限内可追踪、资源的访问和使用不可篡改，为任务执行正确性和计算结果准确性提供佐证。存证内容应包括：

a) 应对各类资源内容或内容摘要进行存证，尤其关键结果数据（或摘要）进行存证，应根据参与方约定保密级别，确保后续通过各方授权在约定期限内能恢复或部分恢复资源内容；

b) 应对各类资源描述信息进行存证，应采用加密、脱敏的方式，对共性信息进行存证，确保该资源后续可被辨识；
c) 应对各类资源的使用日志进行存证，包括资源被资源持有方输入输出、资源更改、资源删除等的行为日志；资源被不同非资源持有方的授权、访问、调用、更新等的行为日志进行存证。

7.4 资源管理

资源管理应包括以下几类：
a) 节点资源管理,节点资源管理的操作包括：初始化节点资源、更新节点资源等；
b) 数据资源管理,数据资源的管理包括：输出/获取数据资源元数据、报告/查询/监测数据资源状态、申请/审核数据资源授权、发布/下线数据资源、更新/删除数据资源、使用/释放数据资源等；
c) 项目资源管理,项目资源的管理包括：创建项目、查询项目、编辑项目、删除项目、添加项目成员等；
d) 组件资源管理,组件资源的管理包括：输出/获取组件资源元数据，报告/查询组件资源状态、申请/审核组件使用授权、发布/下线组件资源、上传/下载组件资源、安装/卸载组件资源、启动/停止组件资源、更新/删除组件资源、使用/释放组件资源；
e) 模型资源管理,模型资源的管理包括：输出/获取模型资源元数据、报告/查询模型资源状态、申请/审核 模型使用授权、发布/下线模型资源、上传/下载模型资源、安装/卸载模型资源、更新/删除模型资源、使用/释放模型资源等。

7.5 资源互联操作

节点之间的资源通过资源认证、获得资源授权、保证数据安全和通信安全的条件下，建立互联关系，以相互提供不同安全级别的资源查询、使用、修改等服务形式进行合作。

7.5.1 资源发布

节点可以通过资源发布接口向平台提交资源发布请求,将认证通过的资源发布在公开的资源列表上，可供其他节点检索和查询。多方安全计算节点可以配置资源发布的可访问范围和用法用量的限制。

表 2 数据资源可访问范围

private	仅限本地节点访问
protect	已签约节点可访问
public	公开可访问

表 3 数据资源的授权使用限制

usage	用途	允许的算法列表 不允许的算法列表
limit	用量	时间限制 数量限制 次数限制

7.5.2 资源发现

节点具备检索并查看其他节点发布的资源信息的能力，如有需要可向该节点发起资源授权申请。

7.5.3 资源授权

节点间需要通过资源授权后才能建立资源连通关系。当节点访问其他节点的某个受保护资源前，被访问资源的归属节点需要对该节点进行资源身份鉴权，没有通过鉴权的资源访问会被拒绝。节点只有通过资源授权，才能获得该资源的访问权限。

7.6 互通接口

7.6.1 数据集互通

数据集互通应包含如下接口，具体接口规范参见附录A：

a) 东西向接口，应包含公开数据集列表查询、数据集明细查询、数据集授权申请、数据集授权意向更新、数据集授权解除、数据集授权状态查询等；
b) 南北向接口，应包含自有数据集创建、自有数据集列表查询、自有数据集信息查询等。

7.6.2 项目互通

项目互通应包含如下接口，具体接口规范参见附录A：

a) 东西向接口，应包含项目审批、项目审批确认、项目审批解除、审批状态查询、项目列表查询、项目信息查询等；
b) 南北向接口，应包含项目创建、项目更新、项目列表查询、项目信息查询等。

7.6.3 模型互通

模型互通应包含如下接口，具体接口规范参见附录A：

a) 东西向接口，应包含合作模型审批、合作模型审批确认、合作模型审批解除、合作模型审批查询等；
b) 南北向接口，应包含模型列表查询、模型信息查询等。

7.7 资源同步

节点应具备资源信息同步接口，以供合作方查询某资源的具体信息和可用状态。

8 算法组件互联要求

8.1 算法组件定义

在多方安全计算互联互通网络中，需要对算法组件和算法流程进行定义来唯一标识算法组件和算法流程：

a) 算法组件应包含的信息项：算法组件标识、算法组件名称、算法组件提供方、算法组件版本号、算法组件功能描述、算法组件通讯协议、算法组件发布日期、组件任务列表、算法输入、算法输出、算法隐私安全性声明、算法组件资源预估、组件编程语言等。其中，算法输入和算法输出应符合数据输入输出规范的要求。算法组件宜包含：组件任务描述、任务协议、任务配置、扩展性信息、当前状态等；
b) 算法流程应包含的信息项：算法流程标识、算法流程名称、算法流程版本号、算法流程功能描述、算法流程的发布日期、流程任务列表、算法流程包含组件信息、算法流程编排方式、算法流程总资源预估等。其中，算法流程宜包含：流程任务描述、任务协议、任务配置、编排方式、扩展性信息、当前运行步骤、当前状态等。

8.2 数据输入输出规范

参与计算任务的合作节点应协商采用统一的算法数据输入输出规范。具体应包含：

a) 数据输入：算法参数、算法数据（算法输入数据的定义）等；
b) 数据输出：报告信息、输出模型，输出数据等。报告信息包括结果模型的评估指标、数据贡献度，结果数据集的统计分布信息等。输出模型是指算法训练迭代得出的模型结果。输出数据包括中间数据和结果数据。

8.3 算法流程编排规范

参与计算任务的合作节点应协商采用统一的算法流程编排方式，包括拓扑顺序任务调度、优先级队列调度、失败任务重试、定时/周期任务、任务操作等功能，应提供多种上下文环境和依赖关系组织形式的支持，灵活调配各个步骤、各个参与方的协作计算过程，实现各个场景下整个任务自动、高效、准时、准确的执行。

8.4 算法组件认证要求

算法组件应通过安全认证机构的认证，保证算法组件的可信性和安全性。

算法组件的安全认证数字证书应包含算法名称、算法描述、算法版本号、有效期、算法隐私安全性声明、开发者签名、安全认证机构签名等，并具有唯一性。算法组件的隐私安全性声明应包含算法安全性定义、算法安全性原理说明、满足安全性的使用规范、使用范围等。

通过认证后的算法组件可部署在多方安全计算平台，宜支持热插拔方式进行算法组件部署。部署在不同多方安全计算平台的算法组件，应在完成基于算法组件的双向认证后，才能进行数据交互，执行多方安全计算互联互通任务。

8.5 算法组件存证要求

算法组件存证指平台应对多方安全计算互联互通任务中的算法组件运行的输入输出和关键操作日志进行记录，以满足后续内外部监管审计，对于违背约定的参与方进行发现、追踪。存证内容应包括：

a) 输入输出存证：应对所有组件和流程的输入输出内容摘要、输入输出参数配置、输入输出时间、输入输出相关方等进行存证；
b) 操作记录存证：应对组件的参数配置、组件提供方和提供时间、组件使用方和使用时间等进行存证；应对流程的编排方式、参数配置、流程执行方和执行时间等进行存证；
c) 任务过程存证：应对组件任务和流程任务的执行过程日志、流程执行方和执行时间等进行存证。

8.6 算法组件流程管理

算法组件流程管理指维持算法组件和算法流程可供正常使用、组件任务和流程任务正常执行的基本能力，应包含：

a) 算法组件管理：包括算法组件的发布、下线、更新、删除、授权申请等；组件任务的列表查询、组件任务启动、禁用、参数修改、输入输出查询等；
b) 算法流程/流程任务管理：包括算法流程的发布、下线、更新、删除、授权申请等；流程任务的列表查询、执行、暂停、参数修改、重新执行、组件重排、输入输出查询等；
c) 算法组件信息和算法流程信息管理：包括算法组件和算法流程信息增加、删除、修改、查询等。

8.7 算法组件互联操作

算法组件间的互联操作包含组件执行、组件停止、组件运行状态获取、运行结果获取等操作。

节点之间应在相互确认算法组件认证、获得算法组件访问授权后，建立算法组件流程的互联关系，通过提前协商的算法组件数据输入输出规范和算法流程编排规范，实现异构平台间跨域协同计算。

8.7.1 算法组件发布

算法组件可以由系统自身提供，也可以由其他系统提供（公开或者半公开的形式）。节点应提前协商算法组件的输入输出数据格式和组件编排顺序，在系统上主动发布算法组件信息，以供其他节点查询调用。

8.7.2 算法组件授权

节点需要得到算法提供节点的授权后，才能将其提供的算法组件加载到本地系统。在必要的情况下，算法提供方应支持取消算法组件的授权。对于已经取消授权的算法组件，系统应具备停用或者卸载能力。

8.7.3 算法组件加载

算法组件应支持以服务常驻模式或者动态拉取模式加载到本地平台，节点应能根据任务的需要来停止算法组件的执行，并完成相关的资源释放和管理。

节点应能主动卸载不需要的算法组件。另外对于已经被吊销证书的算法组件，系统应能识别并卸载。

8.8 互通接口

8.8.1 组件互通

组件互通应包含如下接口，具体接口规范参见附录A：

a） 东西向接口，应包含公开组件列表查询、公开组件信息查询等；

b） 南北向接口，应包含组件注册、组件注销、组件列表查询、组件信息查询等。

8.8.2 流程互通

流程互通应包含如下接口，具体接口规范参见附录A：

a） 东西向接口，应包含流程审批、流程审批确认、流程审批解除、流程状态查询等；

b） 南北向接口，应包含流程创建、流程更新、流程列表查询、流程信息查询、流程删除等。

8.8.3 任务互通

任务互通应包含如下接口，具体接口规范参见附录A：

a） 东西向接口，应包含任务审批、任务审批确认、任务审批解除、审批状态查询等；

b） 南北向接口，应包含任务创建、任务运行、任务停止、任务状态查询、任务日志查询、任务列表查询、任务信息查询等。

8.9 任务同步

本节点应具备定时查询合作节点算法任务的服务状态是否正常的能力。

9 通信协议互联要求

9.1 通信接口

多方安全计算互联互通场景中，通信接口应具备数据安全性、通信完整性和审计安全性，避免数据泄露、防篡改、防攻击、防抵赖。具体分为两类：控制通信，指在各平台之间传输接口控制消息的通信；数据通信，指在各平台底层算法组件之间传输数据的通信。

9.2 通信框架

应采用较为成熟的通信框架，如有实际需求，可针对性地应用新技术通信框架。具体版本和应用层通信协议、RPC 框架、编码方式应由参与厂商共同协商确定。应满足协议分层的要求，各层协议不宜耦合具体的通信框架。

9.3 数据格式

多方安全计算互联互通场景中多方安全计算节点间的通信应采用统一的消息体结构，每个消息体中应包含：

a） head 信息，包含用于校验、标识消息的信息；

b） body 信息，包含传输的消息内容。

9.4 加密机制

数据传输安全层面，应采用 SSL/TLS 的安全机制实现数据通信加密以保证数据传输安全、可靠，通信中用于加密、签名、密钥交换的密码算法的选择应符合国家或国际标准的安全强度要求。

数据防泄露安全层面，应采用成熟的密码学算法或算法框架对参与方原始数据进行加密处理，确保在任何情况下原始业务数据均不会跨节点传输。

9.5 网络环境

多方安全计算互联互通场景中，多方安全计算节点间应通过协商确定网络传输环境，使用一致的网络，运行于公网、内网、运营商专线等物理网络环境之中。

附 录 A
（规范性）
多方安全计算互联互通技术规范互联互通接口

A.1 节点互通

A.1.1 东西向接口

A.1.1.1 节点信息查询

a) 接口描述：发起方查询合作方节点信息。
b) 调用者：发起方
c) 调用方式：GET
d) 接口地址：/v1/interconn/node/query
e) 请求参数

参数	类型	是否必填	描述
node_id	String	是	节点 id

f) 返回参数

参数	类型	是否必填	描述
name	String	是	节点名称
institution	String	是	节点所属机构
inst_id	String	是	机构 Id
system	String	是	技术服务提供系统
system_version	String	是	系统版本
address	String	是	节点服务地址
description	String		节点说明

A.1.1.2 合作申请发起

a) 接口描述：发起方节点向合作方节点发起成为合作伙伴的申请，合作方返回新的合作 id
b) 调用者：发起方
c) 调用方式：POST
d) 接口地址：/v1/interconn/node/contract/apply
e) 请求参数：

参数	类型	是否必填	描述
node_id	String	是	合作方的节点 ID
name	String	是	节点名称
institution	String	是	节点所属机构
inst_id	String	是	机构 Id
system	String	是	技术服务提供系统
system_version	String	是	系统版本

address	String	是	节点服务地址
description	String		节点说明
auth_type	String	是	认证方式，枚举值：SHA256_RSA、SHA256_ECDSA、CERT 等
auth_credential	String	是	凭证内容：公钥值、证书内容等
expired_time	Long		合约过期时间，时区约定 Asia/Shanghai

f) 返回参数

参数	类型	是否必填	描述
contract_id	string	是	合约 id，全局唯一

A.1.1.3 更新合作意向

a) 接口描述：合作方向发起方更新合作意向，包括同意合作申请、拒绝合作申请。
b) 调用者：合作方
c) 调用方式：POST
d) 接口地址：/v1/interconn/node/contract/confirm
e) 请求参数

参数	类型	是否必填	描述
contract_id	String	是	合约 id
status	String		授权状态。枚举值： APPROVED 已授权 REJECTED 已拒绝
auth_type	String	当 staus=APPROVED 时是否必填	认证方式，枚举值：SHA256_RSA、SHA256_ECDSA、CERT 等
auth_credential	String	当 staus=APPROVED 时是否必填	凭证内容：公钥值、证书内容等
expired_time	Long	当 staus=APPROVED 时是否必填	合约过期时间，时区约定 Asia/Shangha

f) 返回参数：无

A.1.1.4 节点合约解除

a) 接口描述：撤销节点间合约关系，双方均可发起。
b) 调用者：发起方/合作方
c) 调用方式：POST
d) 接口地址：/v1/interconn/node/contract/terminate
e) 请求参数

参数	类型	是否必填	描述
contract_id	String	是	合约 id

f) 返回参数：无

A.1.1.5 更新节点信息

a) 接口描述：发起方向合作方同步更新节点信息，更新后合作 id 不变。
b) 调用者：发起方
c) 调用方式：POST
d) 接口地址：/v1/interconn/node/update
e) 请求参数：

参数	类型	是否必填	描述
contract_id	String	是	合约 id
node_info	Node	是	新的节点信息

f) 返回参数：无

A.1.1.6 节点合作查询

a) 接口描述：发起方向合作方查询合作签约状态，确认回调失败的兜底操作
b) 调用者：发起方
c) 调用方式：GET
d) 接口地址：/v1/interconn/node/contract/query
e) 请求参数：

参数	类型	是否必填	描述
contract_id	String	是	合约 id

f) 返回参数：

参数	类型	是否必填	描述
status	String	是	合作状态。枚举值： APPLIED 已申请 APPROVED 已授权 REJECTED 已拒绝 TERMINATED 已解除

A.1.1.7 节点健康探测

a) 接口描述：发起方向合作方进行健康检查
b) 调用者：发起方
c) 调用方式：GET
d) 接口地址：/v1/interconn/node/health
e) 请求参数：

参数	类型	是否必填	描述

f) 返回参数：

参数	类型	是否必填	描述
status	String	是	节点健康状态。直接返

			回 ok

A.1.2 南北向接口

A.1.2.1 节点信息查询

a) 接口描述：发起方向合作方同步更新节点信息，更新后合作 id 不变。
b) 调用方式：GET
c) 接口地址：/v1/platform/node/query
d) 请求参数：

参数	类型	是否必填	描述
node_id	String	是	节点 id

e) 返回参数：

参数	类型	是否必填	描述
node_id	String	是	节点 ID
name	String	是	节点名称
institution	String	是	节点所属机构
inst_id	String	是	机构 Id
system	String	是	技术服务提供系统
system_version	String	是	系统版本
address	String	是	节点服务地址
auth_type	String	是	节点认证方式
auth_credential	String	是	节点凭证
description	String		节点说明

A.1.2.2 节点信息更新

a) 接口描述：更新当前节点信息。
b) 调用方式：POST
c) 接口地址：/v1/platform/node/update
d) 请求参数：

参数	类型	是否必填	描述
node_id	String	是	节点 ID
name	String	是	节点名称
institution	String	是	节点所属机构
inst_id	String	是	机构 Id
system	String	是	技术服务提供系统
system_version	String	是	系统版本
address	String	是	节点服务地址
auth_type	String	是	节点认证方式

auth_credential	String	是	节点凭证
description	String		节点说明

e) 返回参数：无

A.2 数据集互通

A.2.1 东西向接口

A.2.1.1 公开数据集列表查询

a) 接口描述：查询合作方公开的数据集列表
b) 调用方式：GET
c) 调用者：发起方
d) 接口地址：/v1/interconn/dataset/pub/list
e) 请求参数：

参数	类型	是否必填	描述
contract_id	String	是	合约 id
page_num	Integer		页号，默认 1
page_size	Integer		每页数量，默认 20， page_size=-1 时为全量查询

f) 返回参数：

参数	类型	是否必填	描述
total	Integer	是	记录数
records	Array<DatasetSummary>	是	数据集列表

DatasetSummary 参考结构

参数	类型	是否必填	描述
dataset_id	String	是	数据集 ID
name	String	是	数据集名称
description	String		数据集描述（如数据用途、简介等）
count	Integer		样本容量
column_metas	Array<ColumnMeta>		列元数据，与字段排序保持一致。 列表查询时可选，明细查询时是否必填
owner	String	是	数据属主（机构 id）

category	String		数据类别

ColumnMeta 参考结构

参数	类型	是否必填	描述
name	String	是	字段名/特征名
data_type	String	是	字段类型，枚举值：如 varchar、int、double（参考 SQL）
description	String		字段描述
distribution	String	是	数据分布，枚举值：DISCRETE、CONTINUOUS

A.2.1.2 数据集明细查询

a) 接口描述：发起方向合作方查询公开的或已授权的数据集详细信息
b) 调用方式：GET
c) 调用者：发起方
d) 接口地址：/v1/interconn/dataset/pub/query
e) 请求参数：

参数	类型	是否必填	描述
contract_id	String	是	合约 id
dataset_id	String	是	数据集 id

f) 返回参数

参数	类型	是否必填	描述
dataset_id	String	是	数据集 ID
name	String	是	数据集名称
description	String		数据集描述（如数据用途、简介等）
count	Integer		样本容量
column_metas	Array<ColumnMeta>	是	列元数据,与字段排序保持一致。列表查询时可选，明细查询时是否必填。
owner	String	是	数据属主（机构 id）
category	String		数据类别

ColumnMeta 参考结构

参数	类型	是否必填	描述
name	String	是	字段名/特征名
data_type	String	是	字段类型，枚举值：如 varchar、int、double（参考 SQL）
description	String		字段描述
distribution	String	是	数据分布，枚举值：DISCRETE、CONTINUOUS

A.2.1.3 数据集授权申请

a) 接口描述：根据合作方公开数据集 ID 发起授权申请
b) 调用方式：POST
c) 调用者：发起方
d) 接口地址：/v1/interconn/dataset/audit/apply
e) 请求参数

参数	类型	是否必填	描述
contract_id	String	是	合约 id
dataset_id	String	是	数据集 id
time_limit	Long		使用到期时间
audit_id	String	是	审批 id
auth_scope	Array<String>		授权范围类型。 列表中类型取值： NODE 节点级 PROJECT 项目级 COMPONENT 组件级 不填默认节点级
scope_ids	Map<String, Array<String>>		授权适用范围。key 对应 auth_scope，value 为该类型具体的授权对象唯一 id。 如： {“PROJECT”:

			[“project_123”], “COMPONENT”: [“psi”] }

f) 返回参数：无

A.2.1.4 数据集授权意向更新

a) 接口描述：数据集持有方向另一方更新数据授权状态（已申请、已授权、已拒绝）
b) 调用方式：POST
c) 调用者：数据集持有方
d) 接口地址：/v1/interconn/dataset/audit/confirm
e) 请求参数

参数	类型	是否必填	描述
audit_id	String	是	审批 id
status	String		授权状态。枚举值： APPROVED 已授权 REJECTED 已拒绝
resource_permit	ResourcePermit		资源许可凭证

f) 返回参数：无

ResourcePermit 参考结构：

字段名	类型	是否必填	描述
token	String	是	令牌。用于核验的令牌，颁发给资源使用方的唯一授权标识，与授权主体、资源绑定
resource_level	Integer	是	资源等级
resource_type	String	是	资源类型
resource_id	String	是	资源 ID
resourse_node_id	String	是	资源提供方的节点 ID
resourse_inst_id	String	是	资源提供方的机构 ID
request_node_id	String	是	资源使用方的节点 ID
request_inst_id	String	是	资源使用方的机构 ID
time_limit	Long		访问时间限制
times_limit	Integer		访问次数限制

A.2.1.5 数据集授权解除

a) 接口描述：撤销数据集授权权限。
b) 调用者：数据集持有方
c) 调用方式：POST
d) 接口地址：/v1/interconn/dataset/audit/terminate

e) 请求参数

参数	类型	是否必填	描述
audit_id	String	是	授权通过的审批 id

f) 返回参数：无

A.2.1.6 数据集授权状态查询

a) 接口描述：数据集使用方向提供方查询申请状态，确认回调失败的兜底操作。
b) 调用方式：GET
c) 调用者：数据集使用方
d) 接口地址：/v1/interconn/dataset/audit/query
e) 请求参数

参数	类型	是否必填	描述
audit_id	String	是	审批 id

f) 返回参数

参数	类型	是否必填	描述
status	String	是	授权状态。枚举值： APPLIED 已申请 APPROVED 已授权 REJECTED 已拒绝 TERMINATED 已解除

A.2.2 南北向接口

A.2.2.1 自有数据集创建

a) 接口描述：在当前节点创建自有数据集。
b) 调用方式：POST
c) 接口地址：/v1/platform/dataset/create
d) 请求参数：

参数	类型	是否必填	描述
name	String	是	数据名称
description	String		数据描述
source	String	是	数据集来源
location	JSON	是	数据集位置
column_metas	Array<ColumnMeta>	是	列元数据
count	Integer		样本容量
owner	String	是	数据属主
pub_scope	String		数据公开范围
purpose	String		数据用途
category	String		数据类别

e) 返回参数：

参数	类型	是否必填	描述
dataset_id	String	是	数据集 id

A.2.2.2 自有数据集列表查询

a) 接口描述：查询本方节点自有数据集列表
b) 调用方式：GET
c) 接口地址：/v1/platform/dataset/list
d) 请求参数：

参数	类型	是否必填	描述
page_num	Integer		页号，默认 1
page_size	Integer		每页数量，默认 20，page_size=-1 时为全量查询

e) 返回参数：

参数	类型	是否必填	描述
total	Integer	是	记录数
records	Array<Dataset>	是	数据集列表

A.2.2.3 自有数据集信息查询

a) 接口描述：查询本方节点数据集详细信息
b) 调用方式：GET
c) 接口地址：/v1/platform/dataset/query
d) 请求参数：

参数	类型	是否必填	描述
dataset_id	String	是	数据集 id

e) 返回参数

参数	类型	是否必填	描述
dataset_id	String	是	数据 ID
name	String	是	数据名称
description	String		数据集描述
status	Integer	是	状态
source	String		数据集来源
location	Object		数据集位置
column_metas	Array<ColumnMeta>	是	列元数据
count	Integer		样本容量
owner	String	是	数据属主
pub_scope	String		数据公开范围

purpose	String		数据用途
category	String		数据类别

A.3 项目互通

A.3.1 东西向接口

A.3.1.1 项目审批

a) 接口描述：发起方向协作方发起项目审批的请求
b) 调用者：发起方
c) 调用方式：POST
d) 接口地址：/v1/interconn/project/audit/apply
e) 请求参数

参数	类型	是否必填	描述
project_id	Project	是	项目信息
name	String	是	项目名称
description	String		项目描述
type	String		项目类型。枚举值：HOMO_FL、HETERO_FL、MPC…
contract_id	String	是	合约 id
datasets	Array<DatasetSummary>		项目使用的该协作方的数据集
audit_id	String	是	审批 id

f) 返回参数：无

DatasetSummary 参考结构

参数	类型	是否必填	描述
dataset_id	String	是	数据集 ID
name	String	是	数据集名称
description	String		数据集描述（如数据用途、简介等）
count	Integer		样本容量
column_metas	Array<ColumnMeta>	是	列元数据，与字段排序保持一致。分页查询时可省略，单条查询时完整返回

owner	String	是	数据属主（机构 id）
category	String		数据类别

A.3.1.2 项目审批确认

a) 接口描述：合作方向发起方确认审批结果
b) 调用者：合作方
c) 调用方式：POST
d) 接口地址：/v1/interconn/project/audit/confirm
e) 请求参数

参数	类型	是否必填	描述
audit_id	String	是	审批 id
status	String	是	审批状态，枚举值： REJECTED、APPROVED
resource_permit	ResourcePermit		资源许可凭证

f) 返回参数：无

A.3.1.3 项目审批解除

a) 接口描述：撤销已通过的项目审批。
b) 调用者：合作方
c) 调用方式：POST
d) 接口地址：/v1/interconn/project/audit/terminate
e) 请求参数

参数	类型	是否必填	描述
audit_id	String	是	授权通过的审批 id

f) 返回参数：无

A.3.1.4 审批状态查询

a) 接口描述：发起方向合作方查询审批状态，确认回调失败的兜底操作
b) 调用方式：GET
c) 接口地址：/v1/interconn/project/audit/query
d) 请求参数：

参数	类型	是否必填	描述
audit_id	String	是	审批 ID

e) 返回参数：

参数	类型	是否必填	描述
status	String	是	审批状态。 枚举值： APPLIED 已申请 APPROVED 已授权

			REJECTED 已拒绝 TERMINATED 已解除

A.3.1.5 项目列表查询

a) 接口描述：协作方向发起方查询本方参与的项目列表
b) 调用者：协作方
c) 调用方式：GET
d) 接口地址：/v1/interconn/project/list
e) 请求参数

参数	类型	是否必填	描述
page_num	Integer		页号，从 1 开始递增，默认为 1
page_size	Integer		每页查询数据量，默认 20，page_size=-1 时为全量查询
contract_id	String	是	合约 id

f) 返回参数

参数	类型	是否必填	描述
total	Integer	是	数量
records	Array<Project>	是	项目信息列表

A.3.1.6 项目信息查询

a) 接口描述：协作方向发起方查询项目详细信息
b) 调用者：协作方
c) 调用方式：GET
d) 接口地址：/v1/interconn/project/query
e) 请求参数

参数	类型	是否必填	描述
project_id	String	是	project_id
contract_id	String	是	合约 id

f) 返回参数

参数	类型	是否必填	描述
project_id	String	是	项目 id
name	String	是	项目名称
description	String		项目描述
node_ids	Array<Node>	是	合作节点列表
datasets	Map<String, Array<DatasetSummary>>	是	项目使用的数据集。 {“node_id_1”: [“dataset1”，“dataset2”，

			“dataset3”] }
type	String		项目类型

A.3.2 南北向接口

A.3.2.1 项目创建

a) 接口描述：本方节点创建自有项目
b) 调用方式：POST
c) 接口地址：/v1/platform/project/create
d) 请求参数

参数	类型	是否必填	描述
name	String	是	项目名称
description	String		项目描述
contract_ids	Array<String>		合作 id 列表
type	String		项目类型

e) 返回参数

参数	类型	是否必填	描述
project_id	String	是	项目 id

A.3.2.2 项目更新

a) 接口描述：本方节点更新自有项目
b) 调用方式：POST
c) 接口地址：/v1/platform/project/update
d) 请求参数

参数	类型	是否必填	描述
project_id	String	是	项目 id
name	String	是	项目名称
description	String		项目描述
contract_ids	Array<String>		合作 id 列表
type	String		项目类型

e) 返回参数：无

A.3.2.3 自有项目列表查询

a) 接口描述：本方节点查询自有项目列表
b) 调用方式：GET
c) 接口地址：/v1/platform/project/list
d) 请求参数

参数	类型	是否必填	描述
page_num	Integer		页号，默认 1

page_size	Integer		每页数量，默认 20，page_size=-1 时为全量查询

e) 返回参数

参数	类型	是否必填	描述
total	Integer	是	数量
records	Array<Project>	是	项目信息列表

A.3.2.4 自有项目信息查询

a) 接口描述：本方节点查询项目详细信息
b) 调用方式：GET
c) 接口地址：/v1/platform/project/query
d) 请求参数

参数	类型	是否必填	描述
project_id	String	是	project_id

e) 返回参数

参数	类型	是否必填	描述
project_id	String	是	项目 id
name	String	是	项目名称
description	String		项目描述
contract_ids	Array<String>	是	合作 id 列表
type	String		项目类型

A.4 组件互通

A.4.1 东西向接口

A.4.1.1 公开组件列表查询

a) 接口描述：公开可见的组件列表查询。
b) 调用方式：GET
c) 接口地址：/v1/interconn/component/list
d) 请求参数：

参数	类型	是否必填	描述
page_num	Integer		页号，从 1 开始递增，默认为 1
page_size	Integer		每页查询数据量，默认 20，page_size=-1 时为全量查询
developer	String		组件开发者，如：baidu、webank
category	String		非枚举值：LOADER、FEATURE_ENGINEERING…
contract_id	String	是	合约 id

e) 返回参数：

参数	类型	是否必填	描述
total	Integer	是	记录总数
records	Array<ComponentSummary>	是	组件概要信息列表

ComponentSummary数据结构:

参数	类型	是否必填	描述
code	String	是	组件编码
version	String	是	组件版本
developer	String		组件开发者，如：baidu、webank
category	String		枚举值：LOADER、FEATURE_ENGINEERING…

A.4.1.2 公开组件信息查询

a) 接口描述：公开可见的组件信息查询。
b) 调用方式：GET
c) 接口地址：/v1/interconn/component/query
d) 请求参数：

参数	类型	是否必填	描述
code	String	是	组件 code
version	String	是	组件版本
contract_id	String	是	合约 id

e) 返回参数：

参数	类型	是否必填	描述
code	String	是	组件 code，通过一定规范生成
version	String	是	组件版本，如 1.0.0，code 和 version 唯一标识一个组件
name	String	是	组件名称
engine	String	是	组件引擎，如 fate
developer	String		组件开发者，如：baidu、webank
category	String		非枚举值:LOADER、FEATURE_ENGINEERING…
inputs	Array<Object>	是	组件的请求参数定义
outputs	Array<Object>	是	组件的出参定义
extension	Map		扩展信息

status	String	是	枚举值：ENABLED、DISABLED
description	String		组件描述

A.4.2 南北向接口

A.4.2.1 组件注册

a) 接口描述：注册组件相关信息。
b) 调用方式：POST
c) 接口地址：/v1/platform/component/register
d) 请求参数：

参数	类型	是否必填	描述
Component	{Component}	是	组件信息

e) 返回参数：无

A.4.2.2 组件注销

a) 接口描述：注销组件相关信息。
b) 调用方式：POST
c) 接口地址：/v1/platform/component/unregister
d) 请求参数：

参数	类型	是否必填	描述
code	String	是	组件 code
version	String	是	组件版本

e) 返回参数：无

A.4.2.3 组件列表查询

a) 接口描述：组件列表查询
b) 调用方式：GET
c) 接口地址：/v1/platform/component/list
d) 请求参数：

参数	类型	是否必填	描述
page_num	Integer		页号，从 1 开始递增，默认为 1
page_size	Integer		每页查询数据量，默认 20，page_size=-1 时为全量查询
engine	String		组件引擎，如 avatar、fate
category	String		枚举值：LOADER、FEATURE_ENGINEERING…

e) 返回参数：

参数	类型	是否必填	描述
total	Integer	是	记录总数

records	Array<ComponentSummary>	是	组件信息列表

A.4.2.4 组件信息查询

a) 接口描述：组件信息查询。
b) 调用方式：GET
c) 接口地址：/v1/platform/component/query
d) 请求参数：

参数	类型	是否必填	描述
code	String	是	组件 code
version	String	是	组件版本

e) 返回参数：

参数	类型	是否必填	描述
Component	{Component}	是	组件信息

A.5 流程互通

A.5.1 东西向接口

A.5.1.1 流程审批

a) 接口描述：触发合作节点对流程数据进行审批，结果需等待对方通知。
b) 调用方式：POST
c) 接口地址：/v1/interconn/flow/audit/apply
d) 请求参数：

参数	类型	是否必填	描述
project_id	String		项目 ID
name	String	是	流程名称
description	String		流程描述
dag	DAG	是	DAG
config	Config		任务运行时配置
flow_id	String	是	流程 id
audit_id	String	是	审批 id

e) 返回参数：无

A.5.1.2 流程审批确认

a) 接口描述：合作方向发起方确认审批结果。
b) 调用方式：POST
c) 接口地址：/v1/interconn/flow/audit/confirm
d) 请求参数：

参数	类型	是否必填	描述
audit_id	String	是	审批 ID
status	String	是	审批状态，枚举值：REJECTED、APPROVED
resource_permit	ResourcePermit		资源许可凭证

e) 返回参数：无

A.5.1.3 流程审批解除

a) 接口描述：撤销已通过的流程审批。
b) 调用者：合作方
c) 调用方式：POST
d) 接口地址：/v1/interconn/flow/audit/terminate
e) 请求参数

参数	描述	类型	是否必填
audit_id	授权通过的审批 id	String	是

f) 返回参数：无

A.5.1.4 审批状态查询

a) 接口描述：发起方向合作方查询审批状态，确认回调失败的兜底操作
b) 调用方式：GET
c) 接口地址：/v1/interconn/flow/audit/query
d) 请求参数：

参数	类型	是否必填	描述
audit_id	String	是	审批 ID

e) 返回参数：

参数	类型	是否必填	描述
status	String	是	审批状态，枚举值：APPLIED、REJECTED、APPROVED、TERMINATED

A.5.2 南北向接口

A.5.2.1 流程创建

a) 接口描述：创建流程。
b) 调用方式：POST
c) 接口地址：/v1/platform/flow/create
d) 请求参数：

参数	类型	是否必填	描述
project_id	String		项目 ID
name	String	是	流程名称

description	String		流程描述
dag	DAG		DAG
config	Config		任务运行时配置

e) 返回参数：

参数	类型	是否必填	描述
flow_id	String	是	流程 ID，跨节点共享

A.5.2.2 流程更新

a) 接口描述：更新流程，不影响已经在运行的 Job。
b) 调用方式：POST
c) 接口地址：/v1/platform/flow/update
d) 请求参数：

参数	类型	是否必填	描述
flow_id	String	是	流程 ID
name	String		流程名称
description	String		流程描述
dag	DAG		DAG，不填表示不改变
config	Config		任务运行时配置，不填表示不改变

e) 返回参数：无

A.5.2.3 流程删除

a) 接口描述：根据流程标识删除流程。
b) 调用方式：POST
c) 接口地址：/v1/platform/flow/remove
d) 请求参数：

参数	类型	是否必填	描述
flow_id	String	是	流程 ID

e) 返回参数：无

A.5.2.4 流程列表查询

a) 接口描述：流程列表查询。
b) 调用方式：GET
c) 接口地址：/v1/platform/flow/list
d) 请求参数：

参数	类型	是否必填	描述
project_id	String		项目 ID

page_num	Integer		页号，从 1 开始递增，默认为 1
page_size	Integer		每页查询数据量，默认 20，page_size 为 -1 时为全量查询

a) 返回参数：

参数	类型	是否必填	描述
total	Integer	是	记录总数
records	Array<Flow>	是	流程信息列表

A.5.2.5 流程信息查询

a) 接口描述：查询流程信息。
b) 调用方式：GET
c) 接口地址：/v1/platform/flow/query
d) 请求参数：

参数	类型	是否必填	描述
flow_id	String	是	流程 ID

e) 返回参数：

参数	类型	是否必填	描述
Flow	{Flow}	是	流程信息

A.6 任务互通

A.6.1 东西向接口

A.6.1.1 任务审批

a) 接口描述：触发合作节点对任务静态数据进行审批，结果需等待对方通知。
b) 调用方式：POST
c) 接口地址：/v1/interconn/job/audit/apply
d) 请求参数：

参数	类型	是否必填	描述
job_id	String	是	任务 id
project_id	String		项目 ID
flow_id	String	是	所属流程 ID
dag	DAG	是	DAG
config	Config	是	任务运行时参数，包括任务描述信息、关联任务实体、任务配置信息、节点标识、

			角色标识等,在管理面中明确任务参数定义
sync_type	String		节点同步方式
audit_id	String	是	审批 id

e) 返回参数：无

A.6.1.2 任务审批确认

a) 接口描述：合作方向发起方确认审批结果。
b) 调用方式：POST
c) 接口地址：/v1/interconn/job/audit/confirm
d) 请求参数：

参数	类型	是否必填	描述
audit_id	String	是	审批 ID
status	String	是	审批状态，枚举值：REJECTED、APPROVED
resource_permit	ResourcePermit		资源许可凭证

e) 返回参数：无

A.6.1.3 任务审批解除

a) 接口描述：撤销已通过的任务审批。
b) 调用者：合作方
c) 调用方式：POST
d) 接口地址：/v1/interconn/job/audit/terminate
e) 请求参数

参数	类型	是否必填	描述
audit_id	String	是	授权通过的审批 id

f) 返回参数：无

A.6.1.4 审批状态查询

a) 接口描述：发起方向合作方查询审批状态，确认回调失败的兜底操作
b) 调用方式：GET
c) 接口地址：/v1/interconn/job/audit/query
d) 请求参数：

参数	类型	是否必填	描述
audit_id	String	是	审批 ID

e) 返回参数：

参数	类型	是否必填	描述
status	String	是	审批状态，枚举值：APPLIED、REJECTED、

			APPROVED、TERMINATED

A.6.2 南北向接口

A.6.2.1 任务创建

a) 接口描述：创建任务。
b) 调用方式：POST
c) 接口地址：/v1/platform/job/create
d) 请求参数：

参数	类型	是否必填	描述
flow_id	String	是	所属流程 ID
config	Config	是	任务运行时参数，包括任务描述信息、关联任务实体、任务配置信息、节点标识、角色标识等，在管理面中明确任务参数定义
dag	DAG	是	DAG
sync_type	String		信息同步方式：CALLBACK、POLL，为空则默认为 POLL

e) 返回参数：

参数	类型	是否必填	描述
job_id	String	是	任务 ID，跨节点共享

A.6.2.2 任务运行

a) 接口描述：根据任务 ID 启动任务
b) 调用方式：POST
c) 接口地址：/v1/platform/job/start
d) 请求参数：

参数	类型	是否必填	描述
job_id	String	是	任务 ID

e) 返回参数：无

A.6.2.3 任务停止

a) 接口描述：根据任务 ID 停止任务运行
b) 调用方式：POST
c) 接口地址：/v1/platform/job/stop
d) 请求参数：

参数	类型	是否必填	描述
job_id	String	是	任务 ID

e) 返回参数：无

A.6.2.4 任务状态查询

a) 接口描述：查询任务状态
b) 调用方式：GET
c) 接口地址：/v1/platform/job/status/query
d) 请求参数：

参数	类型	是否必填	描述
job_id	String	是	任务 ID

e) 返回参数：

参数	类型	是否必填	描述
status	Map<String, String>	是	任务中所有任务的状态，key 为 task_id，value 为任务的状态，任务状态有 PENDING、RUNNING、SUCCESS、FAILED

A.6.2.5 任务日志查询

a) 接口描述：查询任务日志
b) 调用方式：GET
c) 接口地址：/v1/platform/task/log/query
d) 请求参数：

参数	类型	是否必填	描述
task_id	String	是	任务 ID

e) 返回参数：

参数	类型	是否必填	描述
log_info	String		INFO 日志内容
log_debug	String		DEBUG 日志内容
log_error	String		ERROR 日志内容

A.6.2.6 任务列表查询

a) 接口描述：任务列表查询。
b) 调用方式：GET
c) 接口地址：/v1/platform/job/list
d) 请求参数：

参数	类型	是否必填	描述
project_id	String		项目 ID
flow_id	String		流程 id
page_num	Integer		页号，从 1 开始递增，默认为 1
page_size	Integer		每页查询数据量，默认 20

e) 返回参数：

参数	类型	是否必填	描述
total	Integer	是	记录总数
records	Array<Job>	是	任务信息列表

A.6.2.7 任务信息查询

a) 接口描述：查询任务信息。
b) 调用方式：GET
c) 接口地址：/v1/platform/job/query
d) 请求参数：

参数	类型	是否必填	描述
job_id	String	是	任务 ID

e) 返回参数：

参数	类型	是否必填	描述
job_id	String	是	任务 ID，全局唯一，由调度方生成
flow_id	String	是	所属流程 ID
status	String	是	任务状态，参考值为 PENDING, RUNNING, SUCCESS, FAILED
start_time	Long	是	任务开始时间
finish_time	Long	是	任务结束时间
update_time	Long	是	任务信息更新时间
dag	DAG	是	任务的组件之间组合的配置
config	Config	是	任务运行时的参数配置
priority	Integer		任务优先级。用于排队场景
sync_type	String		节点同步方式。节点间信息同步的方式：CALLBACK（主动回调）、POLL（轮询查询），为空则默认为 POLL

A.7 模型互通

A.7.1 东西向接口

A.7.1.1 合作模型审批

a) 接口描述：触发合作节点对合作模型（碎片）进行审批，结果需等待对方通知。
b) 调用方式：POST
c) 接口地址：/v1/interconn/model/audit/apply
d) 请求参数：

参数	类型	是否必填	描述

model_id	String	是	模型 ID，统一的模型 ID
task_id	String		产生模型的任务
model_ digest	String		模型摘要值
audit_id	String	是	审批 id
apply_project_id	String	是	后续要使用模型的项目 id，非产生模型的项目 id

e) 返回参数：无

A.7.1.2 合作模型审批确认

a) 接口描述：合作方向发起方确认审批结果。
b) 调用方式：POST
c) 接口地址：/v1/interconn/model/audit/confirm
d) 请求参数：

参数	类型	是否必填	描述
audit_id	String	是	审批 ID
status	String	是	审批状态，枚举值：REJECTED、APPROVED
resource_permit	ResourcePermit		资源许可凭证

e) 返回参数：无

A.7.1.3 合作模型审批解除

a) 接口描述：撤销已通过的模型审批。
b) 调用者：合作方
c) 调用方式：POST
d) 接口地址：/v1/interconn/model/audit/terminate
e) 请求参数

参数	描述	类型	是否必填
audit_id	授权通过的审批 id	String	是

f) 返回参数：无

A.7.1.4 合作模型审批查询

a) 接口描述：发起方向合作方查询审批状态，确认回调失败的兜底操作。
b) 调用方式：GET
c) 接口地址：/v1/interconn/model/audit/query
d) 请求参数：

参数	类型	是否必填	描述
audit_id	String	是	审批 ID

e) 返回参数：无

参数	类型	是否必填	描述

status	String	是	审批状态，枚举值：APPLIED、REJECTED、APPROVED、TERMINATED

A.7.2 南北向接口

A.7.2.1 模型列表查询

a) 接口描述：查询当前节点模型，分页接口。
b) 调用方式：GET
c) 接口地址：/v1/platform/model/list
d) 请求参数：

参数	类型	是否必填	描述
project_id	String		项目 ID
page_num	Integer		页号：1、2...，默认 1
page_size	Integer		每页记录数，默认 20

e) 返回参数：

参数	类型	是否必填	描述
total	Integer	是	记录总数
records	Array<Model>	是	数据集信息列表

A.7.2.2 模型信息查询

a) 接口描述：查询当前节点单个模型详情。
b) 调用方式：GET
c) 接口地址：/v1/platform/model/query
d) 请求参数：

参数	类型	是否必填	描述
id	String		模型 ID

e) 返回参数：

参数	类型	是否必填	描述
Model	{Model}	是	数据集信息

参 考 文 献