ICS 03.060
CCS A 11

团　体　标　准

T/BFIA 031—2024

金融业隐私计算互联互通平台技术规范

Technical specification for privacy computing interconnection platform in the financial industry

2024－03－27 发布　　2024－03－27 实施

北京金融科技产业联盟　　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。

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。

本文件由北京金融科技产业联盟归口。

本文件起草单位：北京金融科技产业联盟、中国银联股份有限公司、成方金融信息技术服务有限公司、中国工商银行股份有限公司、上海浦东发展银行股份有限公司、招商银行股份有限公司、深圳前海微众银行股份有限公司、中金金融认证中心有限公司、光大科技有限公司、蚂蚁科技集团股份有限公司、蓝象智联（杭州）科技有限公司、深圳市洞见智慧科技有限公司、上海富数科技有限公司、北京百度网讯科技有限公司、中国农业银行股份有限公司、中国银行股份有限公司、交通银行股份有限公司、中国邮政储蓄银行股份有限公司、中信银行股份有限公司、中国民生银行股份有限公司、兴业银行股份有限公司、浙商银行股份有限公司、华夏银行股份有限公司、浙江网商银行股份有限公司、北京银联金卡科技有限公司、北京国家金融科技认证中心有限公司、建信金融科技有限责任公司、中保科联技术有限责任公司、银联商务股份有限公司、银联数据服务有限公司、中国信息通信研究院、中国电信股份有限公司、中国移动通信集团有限公司、中国联合网络通信有限公司、深圳市腾讯计算机系统有限公司、华为技术有限公司、北京火山引擎科技有限公司、度小满科技（北京）有限公司、深圳壹账通智能科技有限公司、上海荣数信息技术有限公司、同盾科技有限公司、海光信息技术股份有限公司、复旦大学、北京金融信息化研究所有限责任公司、华控清交信息科技（北京）有限公司、北京数牍科技有限公司、北京冲量在线科技有限公司、联易融数字科技集团有限公司、深圳微言科技有限责任公司、北京原语科技有限公司、上海光之树科技有限公司、神州融安数字科技（北京）有限公司、杭州趣链科技有限公司、杭州金智塔科技有限公司、湖南谦川科技有限公司、杭州云象网络技术有限公司。

本文件主要起草人：聂丽琴、黄本涛、李璐、刘宝龙、高鹏飞、周雍恺、李定洲、张远健、丁亚丹、时向一、国钰、郭相林、徐琳玲、刘微、张锦元、许冠、周骏、冯云青、王梦鸽、龚乐诚、刘瑞、傅杰、王思婷、葛明嵩、焦惠芸、范涛、万志辉、邓凯、李松涛、尤萌、黄雅琼、田江、王鹏、王继成、温小芳、周权、张晓蒙、袁鹏程、肖俊贤、阮方圆、陆宇飞、王超、赵可、曾成、王慧敏、马煜翔、姚明、何浩、王湾湾、靳新、赵永坤、卞阳、杨天雅、卫骞、周吉文、陈治宇、于欢、徐安滢、樊明璐、司忠平、张少敏、黄璜、张翼飞、刘玉良、张辉、肖飞军、钱菲、谢谨、王光中、马德辉、邓崇鑫、王心玥、张洪鹏、何鹏、张育涵、刘勇、丁益斌、薛祥杰、高海隆、陈嘉俊、张敬之、曹旭涛、王彦博、陈志豪、董效稳、胡晓龙、王磊、殷山、昌文婷、苏贤朋、胡师阳、邱晓慧、杨波、刘力慷、窦永金、蔡雷、王雪、李武璐、陈海涛、刘志立、费灵、杨劲雄、周璇、李帅、周之恒、章磊、马居朝、白玉真、袁博、杨靖世、章庆、戴锡强、毛万葵、肖坤、李崇、张锦锋、孙林、高峰、李克鹏、陈明、王礼斌、范晓亮、倪琲、李咏、徐旭、吴博峰、刘洋、王聪、龚义成、孙中伟、李泽远、陈鑫、蒋嘉琦、李亚朋、王健宗、黄章成、吴天博、刘立强、赖建章、邓志强、黄翠婷、陈涛、卞杰、应志伟、冯浩、吴杰、叶家炜、夏丽莎、王帅强、鲍思佳、王云河、靳晨、陈璐、金银玉、单进勇、韦晓亚、裴超、宋雨筱、陈浩栋、刘尧、李如先、陈曦、张剑、强锋、吴叶国、马利、李延凯、龚振华、梁栋、张佳辰、于博、刘伟、宁立君、李登峰、徐静、杜静漪、韩梦薇、张豹、朱明杰、郭伟、孟庆洋、黄步添、沈玮、焦颖颖。

金融业隐私计算互联互通平台技术规范

1 范围

本文件给出了金融业基于不同类型隐私计算实现互联互通的平台技术架构、技术要求、安全要求和验证方法。

本文件适用于金融机构开展基于隐私计算的数据合作任务协同需求的设计、开发及应用。

注：本文件中的“隐私计算”类型包括联邦学习、多方安全计算和可信执行环境。

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 35273—2020 信息安全技术 个人信息安全规范

JR/T 0118—2015 金融电子认证规范

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0196—2020 多方安全计算金融应用技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

隐私计算 privacy-preserving computing

隐私保护计算

在保障数据在流通和融合过程中不泄露原始数据的前提下，由两个或多个参与方对分散的数据源进行联合分析计算的一类信息处理技术。

3.2

算法 algorithm

用有限步数求解隐私计算问题的一套明确定义的规则的集合。

[来源：GB/T 11457—2006，2.54，有修改]

3.3

安全算子 secure operator

基于MPC（3.13）、HE等密码技术构建的最小必要计算操作。

3.4

节点 node
机构或组织部署的隐私计算平台产品在实现互联互通时对其他协作方呈现的实体形态。

3.5

数据集 dataset
一个或多个数据提供方参与隐私计算的数据集合。
[来源：JR/T 0196—2020，3.9有修改]

3.6

组件 component
由隐私计算算法、安全算子等封装组成的最小可执行单元。

3.7

任务 task
基于一个组件（3.6）所运行的实例。

3.8

流程 flow
采用DAG结构定义的一组组件（3.6）运行的时序关系。

3.9

作业 job
一个隐私计算流程（3.8）完成运行参数配置后所形成的运行实例，每个运行实例由一组任务（3.7）所构成。

3.10

项目 project
用于管理不同节点（3.4）及数据集（3.5）协作执行同一隐私计算作业（3.9）的载体。

3.11

模型 model
通过隐私计算训练形成的结果实体。

3.12

可信执行环境 trusted execution environment；TEE
基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

注：硬件级隔离是指基于硬件安全扩展机制，通过对计算资源的固定划分或动态共享，保证隔离资源不被富执行环境访问的一种安全机制。

[来源：GB/T 41388—2022，3.3]

3.13

多方安全计算 secure multi-party computation；MPC

一种基于多方数据协同完成计算目标，实现除计算结果及其可推导出的信息之外不泄露各方隐私数据的密码技术。

注：MPC常采用的技术有混淆电路、不经意传输、秘密分享、HE等。

［来源：JR/T 0196—2020，3.1］

3.14

远程验证 remote attestation

一种主机向远程主机证明其硬件和软件环境可信的方法。

［来源：YD/T 4234—2023，3.4］

4 缩略语

下列缩略语适用于本文件。

CONF：配置信息（Configuration）

DAG：有向无环图（Direct Acyclic Graph）

ECDH：椭圆曲线迪菲-赫尔曼（Elliptic Curve Diffie-Hellman）

HE：同态加密（Homomorphic Encryption）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

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

PSI：隐私求交（Private Set Intersection）

SS：秘密分享（Secret Sharing）

5 技术架构

5.1 概述

图 1 隐私计算互联互通平台技术架构

技术架构从支持互联互通模式实现的完整版隐私计算平台角度进行定义。图1给出了互联互通所需的最小必要组成部分，实现功能包括：

a) 管理层：实现对隐私计算平台节点、数据、项目、流程、作业、任务、组件、模型等资源的控制与管理，主要包括各实体相关控制与管理功能模块；
b) 控制层：实现对隐私计算作业与任务的编排管理以及对算法组件的容器化加载管理，主要包括流程调度模块和算法容器管理模块；
c) 算法组件层：实现对算法组件互联协议约定及安全基础计算算子定义，主要包括应用算法组件、安全算子组件和开放算法协议；

注：算法组件层所涉各类算法组件（例如基于 TEE 可信算法组件）可根据具体场景应用需要在图 1 定义的模块组成范围内选择实现。

d) 系统层：实现涉及跨平台、跨模块间标准化通信传输与互联互通计算引擎、存储引擎、TEE构建，主要包括传输模块、计算引擎、存储引擎、TEE、富执行环境。

基于总体框架的节点互通合作形态参见附录A。

5.2 管理层

管理层互通包括：

a) 节点互通管理：约定不同隐私计算平台间的节点发现、签约/解约、信息同步等互联操作的实现路径；
b) 数据互通管理：约定不同隐私计算系统间数据资源的发现、申请、授权、解除授权等互联操作的实现路径；
c) 项目互通管理：约定不同隐私计算平台间的项目创建、合作、信息同步等互联操作的实现路径；
d) 组件互通管理：约定不同隐私计算平台间的组件发现、注册等操作的实现路径；
e) 流程互通管理：约定不同隐私计算平台间的流程创建、授权等操作的实现路径；
f) 作业和任务互通管理：约定不同隐私计算平台间的作业/任务协同运行的实现路径；
g) 模型互通管理：约定不同隐私计算平台间的模型授权、模型使用等互联操作的实现路径；
h) 工作流配置管理：用于描述隐私计算作业运行所需的工作流编排信息和参数配置信息，统一语言描述作业实例运行所需的工作流编排信息和参数配置信息；
i) 授权策略管理：约定了互联互通平台应实现的功能接口，在管理层建立跨平台资源授权与验证机制。

5.3 控制层

5.3.1 流程调度模块

流程调度互通约定各隐私计算参与方协同开展同一隐私计算作业与任务执行的主要流程和接口规范，包括：

a) 作业调度控制：作业调度约定了隐私计算节点间作业管理、查询功能，包含隐私计算协作中作业创建、启动、停止及查询等；
b) 任务调度控制：任务调度约定了隐私计算节点间任务管理、状态同步、查询功能，包含跨平台隐私计算协作中任务启动、停止、回调及查询等。

5.3.2 算法容器管理模块

算法容器管理约定跨平台隐私计算协作中算法容器管理与加载、算法组件注册与发现等功能，包括：

a) 容器管理与加载：用于封装底层容器编排能力，接收调度服务请求、构建算法容器镜像，并支

持将组件的镜像加载为组件实例；

b) 组件注册与发现：为平台提供算法组件实例注册[1)]及管理能力，包括算法组件注册、算法组件发现等。算法组件注册包括瞬时模式和常驻模式[2)]。

5.4 算法组件层

5.4.1 应用算法组件

应用算法组件是基于数据合作任务采用的数据加工计算模块，包括PSI、多方统计、联邦建模、匿踪查询等。

5.4.2 安全算子组件

安全算子组件是基于安全算子的安全基础计算模块，包括：

a) 安全算子服务化接口：对安全算子服务调用方式进行接口化定义，为应用算法组件提供安全基础计算能力。安全算子服务分为有状态服务和无状态服务两种调用方式[3)]；

b) 安全算子表达式：定义安全算子的计算功能，如矩阵乘法、大小比较、计算欧氏距离；

c) 安全算子协议：根据安全算子表达式的功能定义，支持 MPC 协议、全同态、半同态等加密技术实现的安全基础计算算子，一般通过安全算子服务化接口指定具体的协议。

5.4.3 基于 TEE 可信算法组件

可信算法是被TEE保护的所有数据处理算法的总称，包括安全算子和普通明文数据处理算法等。

5.4.4 开放算法协议

5.4.4.1 同构算法互联

同构算法互联约定具有同类型密态数据及中间结果的开放算法协议在平台间协作的流程，包括：

a) 参数获取与校验：用于在算法主体开始执行之前从 5.2 h)工作流配置中获取算法运行所需参数，经过每个参与方合法性校验的过程，示例参见附录 B.1.1；

b) 算法主体运行：参与方通过交换一些中间结果，共同推进算法流程执行得出一个计算结果的过程，参见附录 B.1.2。

5.4.4.2 异构算法互联

异构算法互联约定具有不同类型密态数据或中间结果的开放算法协议在平台间协作的流程，包括。

a) 参数获取与校验：用于从 5.2 h)工作流配置中获取算法运行所需参数，进行合法性校验的过程，示例参见附录 B.2.1；

b) 协议转换：支持不同密码算法保护下的中间计算结果的转换，示例参见附录 B.2.2。

5.5 系统层

5.5.1 计算引擎模块

---

1) 注册是指组件会将自身的描述信息通知给平台，注册后的组件可以用于平台管理及任务调用。发现是指注册的信息可以被平台中其他组件所读取或者查询，用于寻找和定位平台中的已有组件。

2) 瞬时模式是指组件启动后一次性完成指定任务，任务完成后组件即停止运行。常驻模式是指组件启动后持续性对外提供服务，不随任务的完成而停止。

3) 有状态服务是指将一次完整的安全算子服务，拆分为准备、计算、结果获取三个阶段服务，且三个阶段的服务之间具有状态上的关联；无状态服务是指一次性完成安全算子服务，无需安全算子服务来维护服务间状态。

计算引擎为算法容器、安全算子等计算模块提供分布式计算服务。计算引擎提供计算节点横向扩展、分布式计算算力等功能，并以统一接口化调用方式实现计算服务。

5.5.2 存储引擎模块

存储引擎为算法容器、安全算子等计算模块提供分布式存储服务。存储引擎提供存储节点的横向扩展、分布式存储等功能，并以统一接口化调用方式实现存储服务。

5.5.3 传输模块

传输模块约定节点内、节点间的传输接口、报文格式，提供节点内、节点间底层的通信能力。传输模块通过算法组件层的配套传输接口实现传输功能，包括：

a) 传输接口：提供节点间传输接口、容器调用传输接口、传输编程接口；
b) 传输报文约定：提供节点间传输报文、节点间协议转换、容器调用传输报文。

5.5.4 TEE

TEE 为统一远程验证提供运行环境。统一远程验证接口用于屏蔽同构或异构 TEE 中远程验证流程实现的差异。基于 TEE 的隐私计算平台互联互通，包括：

a) 统一远程验证报告生成：主要包含统一远程验证报告内容结构和统一远程验证报告生成接口；
b) 统一远程验证报告校验：主要包含统一远程验证报告校验规则和统一远程验证报告校验接口；
c) 统一验证服务：中心化的 TEE 远程验证统一代理验证服务。

5.5.5 富执行环境

富执行环境提供实现不同类型隐私计算平台间按图 1 完成互联互通所需的计算、存储、传输资源。

6 技术要求

6.1 功能要求

6.1.1 实体元素互通要求

隐私计算互联互通平台应支持实体元素互通与授权策略管理，需要符合下列要求。

a) 节点互通管理：
   1) 加入互联互通中的节点应能查询其他可进行互联互通的节点信息；
   2) 加入互联互通中的节点应能与其他节点建立合作，合作建立后双方相互成为协作方；
   3) 节点间的合作应为非永久性的，签约方应指定合作有效期；
   4) 节点双方在建立合作后，宜具备解除合作的能力；
   5) 当节点信息发生变更时，节点宜将变更信息同步给其他已签约节点。
b) 数据互通管理：
   1) 应支持数据需求方与数据提供方对数据授权、使用等操作进行记录；
   2) 应保证权限最小化原则，满足数据使用的最低要求即可；
   3) 可公开的数据集资源宜支持在节点间互相发现；
   4) 协作方可通过主动授权或申请后授权的方式使用对方允许范围内的数据集资源；
   5) 数据提供方可指定数据有效期、使用范围等授权限定条件，不符合限定条件的数据资源无法使用；数据提供方可在数据授权后取消授权。
c) 项目互通管理：

1） 项目由发起方创建后，应向协作方同步项目信息，协作方宜审批通过后加入项目；
2） 项目发起方宜提前告知协作方该项目计划使用的数据集信息；
3） 项目发起方与协作方宜有项目生命周期管理权限，一方修改后由其他相关方审批。

d) 组件互通管理：
1） 互联互通组件应将组件实体信息正确注册到管理层，平台能解析并保存对应的组件实体信息；
2） 已签约的节点宜支持互相查询对方可用的算法组件列表和信息。

e) 流程互通管理：
1） 互联互通的流程 DAG 应具备统一明确的语义，以实现不同版本 DAG 的相互兼容；
2） 流程 DAG 描述隐私计算工作流中的任务编排信息，宜经过项目协作方授权同意。

f) 作业和任务互通管理：
1） 作业 CONF 描述隐私计算作业运行时参数配置，不同版本的 CONF 应具备统一明确的语义，参与协同隐私计算的各平台调度层应能正确识别、解析作业 CONF；
2） 针对安全管控较严的场景，作业 CONF 宜经项目协作方授权同意。

g) 模型互通管理：
1） 使用模型应获得模型相关方授权同意；
2） 模型使用前宜对模型摘要值进行校验，确保原任务生成的模型与新任务使用的模型一致。

h) 工作流配置管理：
1） DAG 配置应明确组件基本参数信息，正确描述组件名称、标识、版本等信息；
2） DAG 配置应明确输入、输出数据的数据类型及唯一引用标识，正确描述上下游数据依赖关系；
3） CONF 配置应明确作业调度方信息，正确描述作业调度方对应的角色及节点标识；
4） CONF 配置应明确作业参与方信息，正确描述作业参与方对应的角色及节点标识；
5） CONF 配置宜明确作业参数信息，结合参数的应用范围选取恰当的范围标识符，结合作业类型配置适宜的作业参数；
6） CONF 配置宜明确任务参数信息，结合参数的应用范围选取恰当的范围标识符，结合任务运行情况配置适宜的任务参数；
7） 作业参数可包括作业类型、作业申请的 CPU、内存等；
8） 任务参数可包括任务申请的 CPU、内存、组件的算法超参数等。

i) 授权策略管理：
1） 在线授权与访问控制操作，各参与方应建立节点间的双向身份认证；
2） 跨平台资源授权时，各参与方应建立相应的授权凭证与许可凭证；
3） 在资源被访问之前，资源持有方应对资源访问方或资源使用方的身份和授权凭证进行验证；
4） 资源持有方应具备主动取消资源授权的能力；
5） 宜通过令牌关联授权凭证等方式实现资源授权验证；
6） 宜通过撤销授权凭证的方式实现资源授权取消，确保被撤销的凭证范围内的资源无法被访问。

6.1.2 流程调度互通要求

隐私计算互联互通平台应支持流程调度互通功能，需要符合下列要求。

a) 作业调度控制：
1） 平台节点内应支持作业的创建，作业创建的接口应包含唯一的作业编号、算法组件组合的

配置信息、算法组件运行需要的参数配置，可包含节点间任务状态同步的方式；

2) 作业创建完成后，作业创建接口应生成并返回唯一的作业编号；
3) 平台节点内应支持作业的停止和查询，作业的停止和查询接口应包含唯一的作业编号；
4) 应支持跨平台作业创建，作业创建的接口应包含唯一的作业编号、算法组件组合的配置信息、算法组件运行需要的参数配置，可包含节点间任务状态同步的方式；
5) 应支持跨平台作业启动和停止，作业启动和停止的接口应包含唯一的作业编号；
6) 应支持跨平台作业查询，作业查询的接口应包含唯一的作业编号；
7) 跨平台作业状态的定义应满足准备中、运行中、成功、失败的范围。

b) 任务调度控制：

1) 平台节点内应支持查询任务日志，查询任务日志的接口应包含唯一的任务编号、查询的日志类型，可包含查询日志范围；
2) 平台节点内应支持回调任务信息，回调任务信息的接口应包含唯一的任务编号、任务状态；
3) 应支持跨平台任务启动，任务启动的接口应包含唯一的任务编号、任务所属的作业编号和任务对应作业 DAG 中的组件名称；
4) 应支持跨平台任务停止，任务停止的接口应包含唯一的任务编号；
5) 跨平台任务状态的定义应满足准备中、运行中、成功、失败的范围；
6) 应支持跨平台任务状态的同步，并且状态同步的方式应支持主动推送和轮询查询两种；
7) 跨平台任务状态同步的默认方式宜为轮询查询。

6.1.3 算法容器管理要求

隐私计算互联互通平台应支持算法容器管理功能，需要符合下列要求。

a) 算法容器管理与加载：

1) 互联互通平台应按照统一的镜像命名规则、镜像标签定义、工作目录结构、网络通信配置等对算法镜像进行规范化定义；
2) 互联互通平台应按照统一的组件命名规则、组件运行状态、运行日志格式等对组件实例进行规范化定义；
3) 互联互通平台应支持组件实例按常驻或者瞬时形态运行，但组件的工作流程和步骤应保持一致；
4) 应明确算法容器镜像加载机制，平台应通过加载机制，将组件的镜像加载为组件实例，并在常驻形态下将响应接口注册到注册与发现服务上，供任务进行调用；
5) 平台应定期对组件的健康情况进行主动检查，确认组件的健康情况；
6) 瞬时形态下发现组件故障时，平台应主动完成对组件的卸载工作；
7) 上层主动请求组件卸载时，组件管理服务应完成组件容器请求资源的清理，包括临时文件、缓存等；
8) 平台宜对第三方提供的算法镜像提供安全性保护手段，如：摘要值比对、漏洞扫描、签名校验等。

b) 组件注册与发现：

1) 宜明确注册发现流程，注册时间点可在平台初始化时统一注册，在运行中扫描发现组件时动态注册，或者在手工触发时进行注册；
2) 宜配套实现标准化跨平台隐私计算协作组件的注册与发现，注册信息应包含包版本、算法名称、算法参数、参数类型、算法输入、算法输出；
3) 宜明确实现逻辑流程及管理服务流程；
4) 组件注册时应指定瞬时模式或常驻模式，瞬时模式下组件注册可由平台通过静态方式读取

组件镜像上的标签信息，将组件的表述信息传递给平台；常驻模式下组件注册可由组件主动通过接口将注册信息推送给平台，或者提供静态信息被动由平台进行读取。

6.1.4 算法算子组件功能要求

隐私计算互联互通应用算法组件与安全算子组件功能，需要符合下列要求。

a) 应用算法组件：
   1) 应支持容器化打包与部署，并在隐私计算平台上运行；
   2) 应提供配套的算法组件自描述文件，包含算法功能、超参数、输入数据、输出结果等描述信息；
   3) 应在算法组件自描述文件中说明所支持的存储引擎类型及计算引擎类型；
   4) 应支持与控制层通过约定的参数传递规范与算法控制接口实现交互；
   5) 应支持通过本地存储或主流的存储引擎接口实现存储功能；
   6) 应支持通过本地计算或主流的计算引擎接口实现计算功能；
   7) 应支持与传输模块约定接口与报文规范，实现与多方协作通信，完成算法预期功能；
   8) 宜支持处理大数据量输入与输出；
   9) 宜支持算力的水平或垂直扩展，如计算集群或者硬件加速；
   10) 宜明确算法组件实例状态并支持协作方间状态可观测；
   11) 宜支持开放追踪接口以及可监控、可管理的日志实现算法组件实例状态可观测，其中日志包括与算法关联的必要信息，如任务编号、任务执行情况等。

b) 安全算子组件：
   1) 安全算子应满足算法组件的相关要求，并向算法组件层提供明确的功能范围清单；
   2) 安全算子应支持多种安全算子表达式与 MPC 协议组合的计算，提供有状态与无状态服务；
   3) 安全算子表达式定义安全算子的功能范围，应满足安全算子服务化接口边界的定义要求；
   4) 安全算子服务提供方应明确所提供的安全算子表达式范围，并支持对安全算子表达式的扩展；
   5) 安全算子用于 MPC 协议时，应满足 JR/T 0196—2020 中 6 所述要求；
   6) 安全算子宜支持参与方角色制定，并依次完成计算协议处理；
   7) 安全算子宜支持直接向安全算子传值、通过数据存储服务间接处理数据两种数据输入输出模式；
   8) 安全算子宜支持应用算法指定数据的输入与输出格式，包括数据类型与数据块的组织形式；
   9) 安全算子宜支持异步化处理的计算任务功能。采用异步方式处理时，应支持异步方式关闭正在执行的安全算子计算任务；
   10) 安全算子可采用同步方式等待安全算子的处理结果。

常用的应用算法与安全算子见附录 C。

6.1.5 开放算法协议设计

6.1.5.1 同构算法互通要求

完整的同构算法互联技术需要符合下列要求。

a) 参数获取与校验，宜包括：
   1) 算法执行参数；
   2) 算法安全性参数。

b) 算法主体运行，应支持：
   1) 明确协商一致的算法交互流程；
   2) 包含每个阶段程序计算结束的标志和判断逻辑；
   3) 根据实现算法互通需要选择编程使用的框架及具体实现的编程语言。

同构开放算法协议每类算法的接口协议细节可有区别，附录B.1以ECDH-PSI为例给出了同构算法的接口要求参考。

6.1.5.2 异构算法互通要求

完整的异构算法互联技术要点需要符合下列要求。

a) 参数获取与校验，宜包括：
   1) 不同平台所使用的密码类型和相关安全参数；
   2) 算法执行参数；
   3) 协议转换方向。
b) 协议转换：
   1) 应支持不同密码算法保护下的中间计算结果的转换；
   2) 宜支持点对点模式或代理模式。

附录 B.2 以秘密分享与 HE 的异构算法协议转换为例给出了一种典型的密码算法转换协议参考。

6.1.6 统一远程验证报告管理

采用 TEE 隐私计算方案时，隐私计算互联互通平台应支持统一远程验证报告管理，需要符合下列要求。

a) 统一远程报告生成：
   1) 统一远程验证报告生成接口应采用不同的远程验证报告内容结构类型适配不同的使用场景；
   2) 统一远程验证报告生成接口应支持新鲜值防止重放攻击；
   3) 统一远程验证报告生成接口中，TEE 或者可信应用实例的身份标识参数宜使用兼容性较好的数据类型格式；
   4) 统一远程验证报告生成接口宜支持对不同 TEE 的其他差异部分进行参数兼容扩展，可采通用参数定义方案和数据类型格式；
   5) 统一远程验证报告内容结构宜使用便于各种应用之间数据交互的表达格式作为统一远程证明报告内容结构，如 JSON 格式；
   6) 统一远程验证报告内容结构宜采用统一命名规则命名具体的数据项名称。
b) 统一远程验证报告校验：
   1) 统一的远程验证报告校验规则中应含 TEE 系统和可信应用相关所有可被校验属性集合；
   2) 校验方可根据 TEE 系统和应用场景自由选择对应的属性进行校验。
c) 统一证明服务：
   1) 统一验证服务接口应遵循统一格式；
   2) 统一验证服务返回的验证结果应具备统一格式，便于校验端执行其他额外校验；
   3) 各个 TEE 端在交互通信前，向对端发起远程验证请求获取统一远程验证报告，统一远程证明报告的验证可在应用内部完成，也可由统一验证服务代理完成；
   4) 统一验证服务可分为节点注册和节点远程认证两个步骤。

不同 TEE 的远程验证报告内容结构及生成接口应进行统一抽象。统一远程验证报告内容结构参见附录 D.1，统一远程验证报告生成接口形式参见附录 D.2。

不同 TEE 的远程验证报告校验规则应基于被校验的属性集合进行统一抽象，不同 TEE 的远程验证报告校验接口应进行统一抽象。统一远程验证报告校验规则及接口形式参见附录 D.3。

6.1.7 传输管理

隐私计算互联互通平台应支持传输管理，需要符合下列要求。

a) 节点间传输报文应约定传输模块间进行跨域数据传输的报文规范。对基于 HTTP 协议的报文头规范进行描述，参见附录 E.1.1；
b) 节点间传输接口应约定传输模块间进行跨域数据传输的接口规范。对接口规范进行描述，参见附录 E.1.2；
c) 节点间协议转换应约定：
   1) 同步协议转换采用非标准传输协议时，应在节点侧内完成协议转换，该转换应由传输模块处理；
   2) 同步协议转换传输模块应根据协议信息调用协议转换插件的匹配方法，来判断此插件是否生效；
   3) 同步协议转换宜选择 HTTP2.0 作为推荐的标准传输协议，保留 HTTP1.1 与 HTTP3.0 以提供兼容的标准传输协议选项；
   4) 异步协议转换时，节点间宜采用同步传输协议投递消息；
   5) 异步协议转换宜使用传输报文规范中的扩展元数据结构；
   6) 异步协议转换消费者端在接收到同步调用的消息投递后，可自行构建到消息服务器的报文转换。
d) 容器调用传输接口宜约定算法容器调用传输模块的报文和接口规范，接口功能应支持以下内容：
   1) 发送信息，向通信信道中发送数据；
   2) 获取信息，阻塞情况下，从通信信道中读取数据；
   3) 快速查询，非阻塞情况下，从通信信道中读取数据；
   4) 会话释放，可选，释放信道中的一个会话。

   对接口规范进行描述，参见附录E.2。
e) 传输编程接口宜约定传输模块为算法和算子代码所提供的程序接口，宜支持以下内容：
   1) 建立信道，建立用于通信的信道，一个信道可对应多个会话；
   2) 关闭信道，关闭用于通信的信道，即关闭信道中的所有会话；
   3) 发送信息，向通信信道中发送数据；
   4) 获取信息，阻塞情况下，从通信信道中读取数据；
   5) 快速查询，非阻塞情况下，从通信信道中读取数据；
   6) 会话释放，可选，释放信道中的一个会话。

   对接口规范进行描述，参见附录E.3。

6.2 非功能要求

6.2.1 兼容性

隐私计算互联互通平台在兼容性上应满足以下要求：

a) 支持不同操作系统；
b) 支持不同部署环境；
c) 支持不同隐私计算平台技术框架；

d) 支持常见数据引擎与计算引擎；
e) 支持向后兼容；
f) 采用 TEE 互通时，支持不同 CPU 架构及平台硬件。

6.2.2 准确性

基于互联互通执行的隐私计算任务算法准确性指标取值应与非互联互通方式无明显偏差。

6.2.3 可扩展性

隐私计算互联互通平台在参与方、算法、算子、算力等方面应具备可扩展性。在算法互联上，应至少具备算法迁移和开放算法协议其中之一的算法能力。

对于开放算法协议实现的互联互通算法，应支持：

a) 算法本地实现开放；
b) 算法和安全机制扩展；
c) 交互出域信息透明。

6.2.4 高可用性

隐私计算参与方应满足互联互通计算资源节点的高可用。

7 安全要求

7.1 数据安全

隐私计算系统在数据安全方面应满足以下要求：

a) 对涉及个人信息的操作，符合 GB/T 35273—2020 中 9.2 和 JR/T 0171—2020 中 6.1.4.2；
b) 使用符合国家商用密码标准的密码算法和组件，包括但不限于哈希算法、加密算法、签名算法、密钥管理组件等；
c) 确保各个参与方用于互联互通计算的原始数据不对外公开，以保障各隐私计算系统的数据隐私性。

7.2 系统安全

隐私计算系统在系统安全方面需要满足以下要求：

a) 应保证任务计算过程中的数据安全，防止出现数据泄露等问题；
b) 参与互联互通的 TEE 系统宜使用可信启动或安全启动流程保证系统的完整性，使用已证明的可信内核和可信软件，组合形成所需的业务能力。

7.3 传输安全

隐私计算互联互通平台在传输安全方面应采用密码技术满足以下要求：

a) 保证传输过程中数据的完整性、真实性；
b) 保证传输过程中敏感信息的数据字段或报文整体的机密性；
c) 保证网络边界访问控制信息、平台资源访问控制信息的完整性；
d) 保证参与通信的各实体行为的不可抵赖性；
e) 具备在通信延时、中断等异常情况下的处理和恢复机制；

f) 使用密码加密功能实现机密性，保护的对象为传输和存储的核心数据、重要数据、敏感信息数据，身份鉴别信息，密钥数据；
g) 使用数字签名实现完整性，保护的对象为传输和存储的核心数据、重要数据、敏感信息数据，身份鉴别信息，密钥数据；
h) 使用对称加密、动态口令、数字签名等实现真实性，应用场景为通信双方的身份鉴别、平台的身份鉴别；
i) 使用数字签名等技术实现不可抵赖性，针对平台中所有需要无法否认的行为，包括发送、接收、审批等操作；
j) 使用远程验证校验保证参与互联互通的 TEE 间相互信任彼此运行在 TEE 中的可信应用程序计算逻辑，鉴别可信应用程序身份，保证授权操作与安全通信。

7.4 算法算子安全

参与隐私计算跨平台合作的多个参与方，均应根据当下业内实际使用需要，提前协商和确认加载算法包的安全可信性，控制算子的内容和范围。需要满足以下要求：

a) 开放算法协议的算法应保持安全参数的一致性，应保证中间参数数据处于“不可见”状态；
b) 新的算法实现不应对原有平台引入新的安全风险；
c) TEE 应用中应使用业界共识的安全的密码学算法，并给出相关参考；
d) 算子开发方设计的算子应具备安全原子性；
e) 安全算子服务，应具备机密性，应采取有效技术防护措施，防范通过输入、输出或中间数据推算出其他方的敏感信息；
f) 实现安全算子时，涉及多方安全算子部分，应满足 JR/T 0196—2020 中 7；
g) 算子开发方应为安全算子提供可控、可评估的安全保障；
h) 算法组件应支持任务执行前的安全检查与认证功能。

7.5 认证授权

对互联互通任务计算过程中的关键环节进行身份认证与访问控制，确保操作行为的合法性和抗抵赖性。应满足以下要求：

a) 参与联合计算各通信方之间，建立以节点为主体的双向身份认证；
b) 采用数字证书的方式进行节点间的双向身份认证；
c) 数字证书的使用，满足 JR/T 0118—2015 中 6.4；
d) 通过校验资源访问令牌和会话编号等方式对传输模块报文通信进行访问控制。

7.6 安全审计

隐私计算互联互通平台在安全审计方面需要满足以下要求：

a) 应支持管理层各实体元素全生命周期的审计存证，以及每次合作的审批与凭证记录；
b) 宜支持流程调度、数据输入输出以及算法计算过程的可观可测可追溯，具体实践中审计的对象包括但不限于存证和日志。

8 验证方法

8.1 功能验证

功能验证需要满足以下要求。

a) 测试方法：
   1) 查看各合作节点间是否能够在合约有效期内进行数据集、项目、流程等授权审批，并正常开展合作；
   2) 查看是否能使用脚本配置工作流编排信息和参数配置信息；
   3) 尝试是否能够篡改身份认证信息、授权和许可凭证、资源访问令牌等；
   4) 查看算法是否是容器化加载，确认各组件能够读取或查询该算法组件的注册信息；
   5) 查看交互互通的开放算法协议，并按照所确定算法类型执行算法任务，查看算法执行结果；
   6) 通过安全算子接口执行多种安全算子表达式和多种MPC协议的组合计算，确认计算结果；
   7) 查看节点间传输报文和传输接口是否按照本文件约定所实现，确认传输过程使用密码技术保障数据的完整性、真实性和机密性；
   8) 通过统一远程验证流程对TEE系统以及运行在TEE中的可信算法进行安全性校验。
b) 预期结果：
   1) 不同隐私计算平台节点的管理层间在合约有效期内可相互进行数据集、项目、流程等授权审批操作；
   2) 管理层与控制层间的协作遵循 6.1.1h）中要求的内容，脚本使用统一语言描述工作流编排信息和参数配置信息；
   3) 数据授权策略管理遵循 6.1.1i）中要求的内容，包含授权、验签等动作及令牌、凭证等交互；
   4) 算法应以容器化加载形式对外提供服务，其中组件注册与发现符合 6.1.3a）中要求的内容；
   5) 使用开放算法协议遵循 6.1.5 要求的内容，具备参数获取与校验、协议转换等功能，能够实现同构与异构情况下互联的功能；
   6) 安全算子使用或扩展遵循 6.1.4 要求的内容，并支撑实现算法的安全性；
   7) 节点间传输报文编码满足 6.1.7 中要求的内容，采用密码技术支撑传输安全，并符合 7.3 要求的内容；
   8) 统一远程验证报告使用和扩展遵循 6.1.6 要求的内容。
c) 结果判定：
   实际判定结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

8.2 非功能验证

非功能验证需要满足以下要求。

a) 测试方法：
   1) 查阅相关文档，查看节点平台是否能够做到对不同操作系统、部署环境、技术框架、常见数据系统及硬件的兼容性；
   2) 查看隐私计算任务算法是否能做到与非互联互通方式无明显偏差；
   3) 查看节点平台部署实现方案，确认是否在参与方、算法、算子、算力等方面具备可扩展性；
   4) 查看互联互通计算资源节点方案是否能够实现高可用。
b) 预期结果：
   1) 兼容性符合 6.2.1 节要求的内容；
   2) 准确性符合 6.2.2 节要求的内容；
   3) 可扩展性符合 6.2.3 节要求的内容；
   4) 高可用性满足 6.2.4 节要求的内容。
c) 结果判定：
   实际判定结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

附 录 A
（资料性）
节点合作形态示例

隐私计算互联互通平台间协作涉及从管理面到数据面的互通。管理面互通是指对管理层所属各类互联互通实体元素及授权策略信息的对齐与同步。数据面互通是指管理面下发作业任务后，所涉及的流程互通调度、隐私计算算法组件运行启动、系统环境等各层面的互通对齐。

实际互联互通合作中，各合作节点的隐私计算平台只要按照本文件要求对互联互通相关接口实现，在形态上可以存在一定差异，例如金融机构A（节点1）和金融机构B（节点2）遵循本文件对管理层、控制层、算法组件层、系统层所涉各项要求对自有平台进行了改造，则节点1和节点2可按照互联互通相关接口协作执行同一隐私计算任务。金融机构C（节点3）的隐私计算平台暂时不具备管理面，则其可在数据面按照本文件进行改造的基础上，通过命令行等形式完成工作流配置与授权策略同步等操作，并与节点1/节点2进行协作。关于参与互联互通合作的各节点间形态与交互流程可参考图A.1。

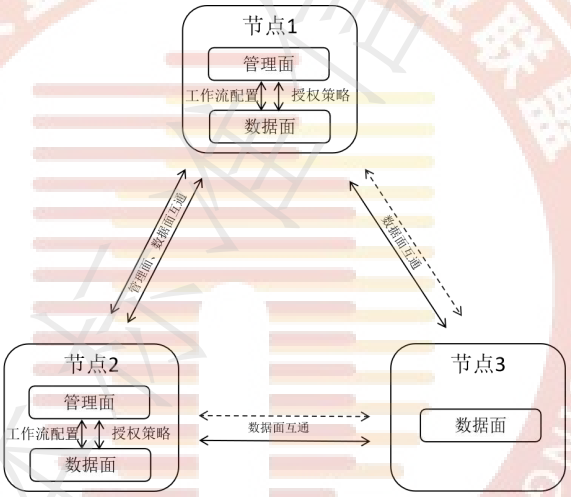

图 A.1 互联互通节点合作形态

注1：根据实际合作节点形态，上述任一节点也可能作为另一网络形态的中心节点进行接入。

注2：参与方各节点以各方都具备管理面与数据面的同构形态为主（如节点1和节点2），特殊情况下部分异构节点可能仅使用数据面参与互通及执行隐私计算任务（如节点3）。

注3：根据实际合作节点形态，任一节点也可能作为另一网络形态的中心节点进行接入。

注4：各节点间协作还将涉及管理面管理信息同步，管理面与数据面间工作流配置与资源授权，数据面流程调度、作业任务启停、算法算子运行、数据传输以及TEE参与互通模式下的统一远程验证等主要流程。

附 录 B
（资料性）
开放算法协议示例

B.1 基于ECDH-PSI的同构算法接口协议

B.1.1 参数获取与校验

算法任务执行前，需要接收任务运行所需的参数并进行格式校验，同构算法参数具体内容见表 B.1。

表 B.1 同构算法参数配置列表

属性名称	数据类型	数据说明	示例	数据备注
version	int32	约定算法的版本号	2	必选
algo	int32	支持的 PSI 算法的枚举值，ECDH-PSI 算法固定为 1	1	必选
protocol_families	int32 list	支持的协议族的枚举值，ECDH-PSI 所需的 ECC 协议族固定为 1	[1]	必选
protocol_family_params	google.protobuf.Any list	相应的协议族详细配置参数，ECC 协议族的类型是 EccProtocolResult	见表 B.2	必选
io_param	google.protobuf.Any	PSI 算法的输入和结果输出格式参数，ECDH-PSI 协议的类型是 PsiDataIoResult	见表 B.3	必选
注：为了使合作方准确识别算法，建议在 DAG 中完整填写算法信息。算法参数通过算法组件自描述文件传递。				

其中 EccProtocolResult 包括 ECDH-PSI 算法参数的基本信息，如表 B.2。

表 B.2 EccProtocolResult 参数配置列表

属性名称	数据类型	数据说明	示例	数据备注
version	int32	ECC 参数格式的版本号	1	必选
ec_suit	tuple <int32,int32,int32>	算法套件编号，由三元组 <Curve 编号, Hash 编号, HashToCurveStrategy 编号>组成	<2,1,1> 其中：2=SM2, 1=SM3, 1=TRY_AND_INCREMENT	必选
point_octet_format	int32	椭圆曲线点的序列化格式的编号	2 其中： 2=X962_COMPRESSED	必选
bit_length_after_truncated	int32	二次密文截断选项，二次密文长度超过该比特数后执行截断，用于减少网络通信量。-1 表示不截断	30 即二次密文最多保留 30 bits 长度	必选

PsiDataIoResult 包括输入输出参数协商的基本信息，如表 B.3。

表 B.3 PsiDataIoResult 参数配置列表

属性名称	数据类型	数据说明	示例	数据备注
version	int32	IO 参数格式的版本号	1	必选
item_num	int64	待求交的 PSI 数据总量	10000	可选

表 B.3 （续）

属性名称	数据类型	数据说明	示例	数据备注
result_to_rank	int32	指定 PSI 结果获取方，填写参与方的 rank 编号。-1 表示所有参与方都可以拿到结果。	-1	必选

B.1.2 算法主体运行

算法主体运行阶段，EcdhPsiCipherBatch 用于传递一次加密后的密文和二次加密后的密文，其参数配置列表如表 B.4 所示。

表 B.4 EcdhPsiCipherBatch 参数配置列表

属性名称	数据类型	数据说明	示例	数据备注
type	string	标识密文的类型，“enc”表示一次加密点，“dual.enc” b 表示二次加密点	“enc”	必选
batch_index	int32	传输批次的编号。当待求交集合较大时，发送方可选择分多个批次发送密文	0	必选
is_last_batch	bool	是否为最后一个传输批次	false	必选
count	int32	当前批次包含的密文数量	1000	必选
ciphertext	bytes	当前批次包含的密文	-	必选
注：参数配置列表仅为报文内容，实际执行时需结合节点传输协议添加报头。				

B.2 秘密分享与HE的异构算法协议转换

B.2.1 参数获取与校验

以代理部署模式为例，在任务执行前，各系统需要先接收任务运行所需的参数并进行格式校验。参数信息包括版本、算法提供方标识信息、算法模块、算法名称、详细算法参数。

B.2.2 协议转换

在任务执行过程中交互数据时，各系统向转换实例送密文数据包，经该实例转换后，再将数据包发送到下一跳目标系统上。交互转换数据结构见表B.5。

表 B.5 交互转换数据结构

属性名称	数据类型	数据说明	数据备注
encryption_type	string	加密类型，例如 SS4、HE 等	必选
shape	tuple	数据形状	必选
data_type	int32	数据类型，例如字符串、矩阵、多维数组等	必选
data	bytes list	密文数据	必选
process	int32 list	数据转换过程，例如 HE_2_SS、SS_2_HE	必选
key	string	密钥或其他安全参数	可选

表 B.5 （续）

属性名称	数据类型	数据说明	数据备注
batch_count	int	该批次总包数	必选
batch_id	string	批次号	必选

附 录 C
（资料性）
常用应用算法与安全算子

表C.1列出了跨隐私计算平台开展数据合作时常用的隐私计算算法与算子。

表C.1 常用算法与算子

名称	类型	说明	示例
算法	线性回归算法	利用传统线性回归概念来拓展和扩展可用其他数据分布，而不仅仅是正态分布，与传统线性回归不同，这种拓展可以处理非正态分布的回归模型。包括一般线性回归算法和广义线性回归算法。	逻辑回归、线性回归、泊松回归、Gamma回归、Tweedie回归
	树结构算法	一种将层次结构式的构造性质，以图象方式表现出来的方法，以树的象征来表现出构造之间的关系，在呈现上是一棵上下颠倒的树，其根部在上方，而下方的内容称为枝干与叶子。	XGBoost、轻量梯度提升机、梯度提升决策树、随机森林
算子	基本算子	主要是指四则运算的算子类型	加、减、乘、除
	复杂算子	主要是指基于基本运算或隐私计算技术实现的复杂运算的算子类型。	平方、平方根、方差、求和、均值、分位数、幂运算、指数运算
	比较算子	主要是指进行数据比较运算的算子类型。	大于、大于等于、小于、小于等于、等于
	逻辑算子	主要是指进行数据逻辑运算的算子类型。	与、或、非、异或
	矩阵算子	主要是指对矩阵类型、向量类型数据运算的算子类型。	矩阵加减乘、向量运算

附 录 D
（资料性）
统一远程验证报告生成模块示例

D.1 统一远程验证报告内容结构

统一远程验证报告内容结构是为屏蔽不同类型 TEE 中远程验证报告内容结构差异所定义的统一抽象式表达，参见表 D.1。

表D.1 统一远程验证报告内容结构

格式说明	名称	类型	必选	说明
对象名称	UnifiedAttestationReport			
字段名称	str_report_version	string	是	当前统一远程报告遵守的格式规范版本号
	str_report_type	string	是	报告的类型格式，可选值如下： BackgroundCheck：背调模式 Passport：护照模式 Uas：统一证明服务器代理模式
	str_tee_platform	string	是	TEE系统标识名称
	json_report	string	是	序列化过的不同TEE系统内容特定报告内容
	json_nested_reports	string	否	JSON序列化之后的UnifiedAttestationNestedReports格式嵌入子报告
对象名称	UnifiedAttestationNestedReports			
字段名称	json_nested_results	string	是	JSON序列化之后的UnifiedAttestationNestedResults格式子报告校验结果集合
	b64_nested_signature	string	是	主报告生成方签名的子报告结果集合签名值
对象名称	UnifiedAttestationNestedResults			
字段名称	nested_report_results	对象列表	是	UnifiedAttestationAttributes属性集对象列表，每一项对应一个子报告校验结果。

D.2 统一远程验证报告生成

统一远程验证报告生成接口参见表D.2。

表D.2 统一远程验证报告生成接口

接口名称	UnifiedAttestationGenerateReport			
接口声明	名称	类型	必选	说明
请求参数	tee_identity	const char*	是	TEE或者可信应用实例的身份标识
	report_type	const char*	是	报告的类型格式，可选值如下： BackgroundCheck：背调模式 Passport：护照模式 Uas：统一验证服务器代理模式
	report_hex_nonce	const char*	否	用户定义的报告新鲜值，不超过64字节的hex编码字符串
	report_params_buf	const char*	否	其他不同TEE系统自定义参数字段地址
	report_params_len	unsigned int	否	其他不同TEE系统自定义参数字段长度
	report_json_len	unsigned int*	是	报告字段最大可接收长度

表 D.2 （续）

返回值	-	int	是	0：成功 其他：十六进制错误编码
	report_json_buf	char*	是	用于存放生成的JSON序列化的统一远程验证报告字符串的报告字段地址
	report_json_len	unsigned int*	是	报告字符串实际长度
注：report_params表示报告的参数。				

D.3 统一远程验证报告校验

统一远程验证报告校验规则是针对统一远程验证报告内容结构相关校验规则的抽象式表达，参见表D.3。

表D.3 统一远程验证报告校验规则JSON格式

格式说明	名称	类型	必选	说明
对象名称	UnifiedAttestationPolicy			
字段名称	pem_public_Key	string	否	pem格式公钥，一般报告里面包含公钥HASH的时候，需要提供该公钥原文用于验证公钥安全
	main_attributes	对象列表	是	UnifiedAttestationAttributes属性集对象列表，至少包含一个用于主报告校验的属性集，多个属性集表示主报告通过任意一项属性集校验即可。
	nested_policies	对象列表	否	NestedPolicies格式对象列表，对象总数和顺序和主报告包含的嵌套子报告总数和顺序对应。
对象名称	NestedPolicies			
字段名称	sub_attributes	对象列表	是	UnifiedAttestationAttributes属性集对象列表，至少包含一个用于子报告校验的属性集，多个属性集表示子报告通过任意一项属性集校验即可。

统一远程验证报告校验相关接口可参见表 D.4。

表D.4 统一远程验证报告校验接口

接口名称	UnifiedAttestationVerifyReport			
接口声明	名称	类型	必选	说明
请求参数	report_json_str	const char*	是	JSON序列化的统一远程证明报告地址
	report_json_len	unsigned int	是	JSON序列化的统一远程证明报告长度
	policy_json_str	const char*	是	JSON序列化的统一远程证明报告校验规则地址
	policy_json_len	unsigned int	是	JSON 序列化的统一远程证明报告校验规则长度
返回值	-	int	是	0：成功； 其他：十六进制错误编码

附 录 E
（资料性）
互联互通接口协议示例

E.1 节点间传输接口协议

E.1.1 节点间传输报文头

节点间报文头携带通信元数据，具体内容见表E.1。

表E.1 节点间传输报文头定义

编码	名称	必选	说明
x-ptp-version	版本	是	协议版本号
x-ptp-tech-provider-code	厂商编码	是	互联互通厂商编码
x-ptp-trace-id	追踪编号	是	全链路追踪编号
x-ptp-token	令牌	是	资源访问控制令牌
x-ptp-source-node-id	发送方节点编号	是	发送端物理节点编号
x-ptp-target-node-id	接收端节点编号	是	接收端物理节点编号
x-ptp-source-inst-id	发送端机构编号	否	发送端业务实体编号
x-ptp-target-inst-id	接收端机构编号	否	接收端业务实体编号
x-ptp-session-id	会话编号	是	全网唯一，用于建立有状态会话的通信，和对 token 的有效性验证

E.1.2 节点间传输接口

节点间通信提供非流式调用和流式调用两种模式，具体内容见表E.2。

表E.2 节点间传输接口定义

传输方式	方法名	传输主体	类型	说明
非流式传输	invoke	请求头	-	见附表 E.1
		请求体	byte	透传二进制报文，不做特殊处理
		响应体		
流式传输	transport	请求头	-	见附表 E.1
		请求体	byte	透传二进制报文，不做特殊处理
		响应体		

E.2 容器调用传输模块接口

容器调用传输模块接口包含发送信息、获取信息、快速查询、会话释放，具体内容见表E.3。

表E.3　容器调用传输模块接口定义

方法	方法名	参数	参数名	类型	必选	说明
发送信息	push	请求参数	payload	byte[]	是	消息序列化后的字节数组
			topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
			metadata	Dict	否	保留参数，用于扩展性
		返回参数	code	string	是	状态码
			message	string	是	状态说明
获取信息	pop	请求参数	topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
			timeout	int	否	超时时间，超出指定时间则立即返回
		返回参数	code	string	是	状态码
			message	string	是	状态说明
			content	byte[]	否	消息序列化后的字节数组
快速查询［可选］	peek	请求参数	topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
		返回参数	code	string	是	状态码
			message	string	是	状态说明
			content	byte[]	否	消息序列化后的字节数组
会话释放［可选］	release	请求参数	topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
		返回参数	code	string	是	状态码
			message	string	是	状态说明

E.3 传输编程接口

传输编程接口包括建立信道、关闭信道、发送信息、获取信息、快速查询、会话释放，具体内容见表E.4。

表 E.4　传输编程接口定义

方法	方法名	参数	参数名	类型	必选	说明
建立信道	open	请求参数	session_id	string	是	信道会话 ID，用于通信的信道隔离
		返回参数	metadata	Dict	是	信道元数据，用于传递开启信道的关键字段
			session	Session	是	信道会话句柄，用于通信传输
关闭信道	close	请求参数	timeout	int	否	超时时间
		返回参数	code	string	是	状态码
			message	string	是	状态说明

表 E.4 （续）

方法	方法名	参数	参数名	类型	必选	说明
发送信息	push	请求参数	payload	byte[]	是	消息序列化后的字节数组
			topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
			metadata	Dict	否	保留参数，用于扩展性
		返回参数	code	string	是	状态码
			message	string	是	状态说明
获取信息	pop	请求参数	topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
			timeout	int	否	超时时间，超出指定时间则立即返回
		返回参数	code	string	是	状态码
			message	string	是	状态说明
			content	byte[]	否	消息序列化后的字节数组
快速查询［可选］	peek	请求参数	topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
		返回参数	code	string	是	状态码
			message	string	是	状态说明
			content	byte[]	否	消息序列化后的字节数组
会话释放［可选］	release	请求参数	topic	string	否	会话主题，相同信道具有唯一性，用于同一信道的传输隔离
		返回参数	code	string	是	状态码
			message	string	是	状态说明

参 考 文 献

[1] GB/T 41388—2022 信息安全技术 可信执行环境系统架构
[2] GB/T 11457—2006 信息技术 软件工程术语
[3] YD/T 4234—2023 基于可信执行环境的安全计算系统技术框架