ICS 35.240.99
CCS L67

T/CCIASC

中 国 计 算 机 行 业 协 会 团 体 标 准

T/CCIASC 0024—2024

多方安全计算互联互通应用评价规范

Evaluation Criteria for Interoperable Multi-Party Secure Computation Applications

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、国网重庆市电力公司电力科学研究院。

本文件主要起草人：齐伟钢、刘从祥、陈建林、郭潇、包佳奇、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、王浩、李其然、韩毅斌、张振威、吴碧莹、孙玉龙、方宏伟、王安宇、黄泰榕、唐刚、张德馨、张浩男、李尤、 刘南嘉、陈柯润、李洋。

引　言

随着多方安全计算技术的发展，异构平台间的互联互通问题日益突出。虽然有相关异构平台互联互通标准的发布，但如何衡量平台的互联互通能力和等级、如何指导用户选型的问题依然存在。因此，制定多方安全计算互联互通应用评价规范和标准很有必要。本标准通过对多方安全计算平台互联互通应用评价提供规范和要求，为互联互通能力评价和用户平台选型提供参考依据。

多方安全计算互联互通应用评价规范

1 范围

本文件规定了多方安全计算互联互通应用评价的术语和定义、评价目的、评价原则、评价资格要求、评价方式、评价方法、评价内容、评价流程和评价等级等。

本文件适用于为多方安全计算互联互通的第三方应用评价提供参考依据。

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 评价目的

a) 通过评价多方安全计算平台的节点互通、数据集互通、项目互通、组件互通、流程互通、任务互通、模型互通等互联互通接口，体现多方安全计算平台在异构平台互联互通领域的能力等级，为多方安全计算互联互通的第三方应用评价提供参考依据。
b) 从供应商角度来看，共性的评价规范能够有效促进厂商之间的有序发展，建立行业的技术门槛，提升供应商的服务能力。
c) 从市场用户角度来看，共性的评价规范能够帮助用户理解各厂商多方安全计算平台技术特点与平台互联互通能力等级，便于用户平台选型。

6 评价原则

a) 公正性，评价活动应不受外界干扰，能独立自主开展评价活动，并形成评价结果。
b) 客观性，评价结果基于客观的证据和事实进行分析，真实、准确地反映评价对象的实际情况。评价指标、评判标准、程序和方法应公正合理 。
c) 综合性，综合考虑多个方面的指标和要求，全面反映多方安全计算互联互通能力等级。
d) 可重复性，评价过程具备可重复性，即在相同条件下可以得到相同的评价结果 。
e) 可靠性，评价应考虑应用的可靠性和稳定性，包括容错能力、可恢复性、应急响应等 。
f) 隐私保护，评价应关注应用对数据的隐私保护，需要基于隐私计算技术实现互联互通。

7 评价资格要求

7.1 评价机构资格要求

评价机构应符合以下要求：

a) 应是独立的法人机构，能够对所做出的评价结论负责，具有提供评价服务所必需的基础设施与工作环境；
b) 拥有一定数量具备多方安全计算互联互通评价能力的评价人员，且不与委托方、成果所有方存在影响评价公正性的关联关系；
c) 不得公开评价过程中的非公开信息。

7.2 评价人员资格要求

评价人员应符合以下要求：

a) 应具备与多方安全计算互联互通评价相关的知识和技能；
b) 不得与委托方或成果所有方存在影响评价公正性的关联关系；
c) 不得公开评价过程中的非公开信息；
d) 应遵纪守法、敬业诚信、客观公正，遵守多方安全计算互联互通评价行业行为规范。

8 评价方式

在多方安全计算互联互通应用的评价过程中，为确保评价的全面性、客观性和科学性，采用的评价方式主要有，委托第三方评价、客户自我评价和综合评价三种评价方式，客户可根据自身情况采取一种评价方式进行评价。

a) 委托第三方评价，旨在借助独立专业机构的权威性和客观性，为多方安全计算互联互通应用提供公正、可信的评价结果。这种方式有助于提升评价结果的公信力，增强各方参与者的信任。
b) 客户自我评价，主要通过组织内部的专业团队进行系统的评估，能够快速发现问题并制定改进措施。此方式具有灵活性和成本效益，能够充分利用客户对自身应用的深入了解优势。
c) 综合评价，该评价方式结合了第三方评价和客户自我评价的优点，能够提供更全面、深入的评价结果。这种方式不仅确保了评价的客观性，还充分利用了客户的内部知识和专业能力，形成更加立体的评估体系。

9 评价方法

9.1 概述

评价方法包括评价工具选择、异构平台部署与配置、互联互通接口验证。

9.2 评价工具选择

在进行评价时，应选择适合的工具以支持数据收集、分析和报告生成。常用的工具包括：

—— 数据包分析工具，如 Wireshark、pcap4j，用于网络通信过程中数据包的捕获和分析；
—— 安全性测试工具，如 OWASP ZAP、Burp Suite，用于识别安全漏洞和潜在风险；
—— 数据分析工具，如 ELK Stack（Elasticsearch, Logstash, Kibana）或 Grafana，用于实时日志数据监测和分析。

9.3 异构平台部署与配置

为了全面评估多方安全计算互联互通能力，应部署两套异构多方安全计算平台，并在每个平台上分别安装必要的中间件、数据库和依赖包，确保环境一致性。根据互联互通接口标准，配置两套平台间的网络策略、通信协议和数据格式，确保能进行有效的数据交换。

9.4 互联互通接口验证

针对每个互联互通接口，进行逐一测试，检查接口的互通性、数据传输的准确性和实时性。

10 评价流程

10.1 概述

评价流程包括申请、受理、组织评价、编制报告、交付报告、后续服务等活动，具体流程见附录 A。

10.2 申请

评价申请由委托方自愿提出，并提交申请评价材料。申请评价材料应包括但不限于以下内容，并按照顺序排列成册:

a) 平台专利、软件著作权等技术报告证明材料；
b) 评价指标要求提供的证明材料；
c) 异构平台互联互通案例证明材料；
d) 其它必要的证明材料。

10.3 受理

受理流程主要包含：

a) 形式审查，如果评价材料齐全且符合要求，评价机构予以受理，否则不予受理；
b) 合同签订，确定受理评价材料后，评价机构应与委托方签订多方安全计算互联互通应用评价咨询合同，明确评价要求，包括评价目的、评价内容、评价依据、评价范围、评价时限、评价费用、保密要求和违约责任等。

10.4 组织评价

组织评价流程主要包含：

a) 评价机构应根据多方安全计算互联互通应用评价特点和评价要求，从人员库中随机抽选人员组成评价委员会，在评价合同签订后 30 个工作日内组织评价委员会开展评价；
b) 采用会议评价形式为主，通过书面审查有关技术资料，对提交材料质询讨论后作出评价结论。必要时可以采用现场或视频答辩、电话咨询、现场测试等方法；
c) 评价委员会应开展审查材料、听取汇报、质询答疑、打分、评价结论讨论等工作。评价结论应经评价委员会一致通过，并由评价人员签字。评价人员应负责会议记录、汇总评价分数、起草初步评价结论和评价报告编写等工作。

10.5 编制报告

编制报告流程主要包含：

a) 评价结束后，评价机构应在 15 个工作日内编制评价报告，评价报告模板参见附录 B；
b) 评价结论包括分项结论和综合结论。分项结论应明确每项指标的评价分值和评价意见。综合结论应对分项结论进行概括分析，提出综合评价意见，确定综合评价分值和评价等级；
c) 评价报告应由评价人员签字，评价机构出具后盖章，并通知委托方。

10.6 交付报告

按照合同约定的时间和方式，评价机构将加盖公章后的评价报告、评价证书交付给委托方。

10.7 后续服务

评价机构应妥善处理委托方或其它相关方关于评价报告内容提出的疑问、异议或申诉。

11 评价内容

多方安全计算互联互通评价主要以《多方安全计算互联互通技术规范 附录A》中互联互通接口为评价指标进行评分，并增加了数据安全性和结果正确性两项指标。在评价过程中，每项指标的评价应以相应指标证明材料为依据，且证明材料宜为公开发布的或第三方机构出具的书面材料，将每项进行分项量化赋分，并汇总得出总分和评价等级。

表 1 多方安全计算互联互通评价指标

指标分类及分值	评价要点	证明材料
节点互通 9 分	**东西向接口：**节点信息查询、合作申请、更新合作意向、节点合约解除、更新节点信息、节点合作查询、节点健康探测是否互通； **南北向接口：**节点信息查询、节点信息更新是否互通； 每个接口互通计 1 分，无法互通计 0 分。本项最多计 9 分。	系统架构设计文档、节点互通详细设计文档、节点互通接口设计文档及代码样例、测试记录报告、异构平台互联互通合作协议及节点互通运行信息，不限于运行日志、页面截图等。
数据集互通 9 分	**东西向接口：**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是否互通； **南北向接口：**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是否互通； 每个接口互通计 1 分，无法互通计 0 分。本项最多计 9 分。	系统架构设计文档、数据集互通详细设计文档、数据集互通接口设计文档及代码样例、测试记录报告、异构平台互联互通合作协议及数据集互通运行信息，不限于运行日志、页面截图等。
项目互通 10 分	**东西向接口：**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、项目信息查询是否互通； **南北向接口：**项目创建、项目更新、自有项目列表查询、自有项目信息查询是否互通； 每个接口互通计 1 分，无法互通计 0 分。本项最多计 10 分。	系统架构设计文档、项目互通详细设计文档、项目互通接口设计文档及代码样例、测试记录报告、异构平台互联互通合作协议及项目互通运行信息，不限于运行日志、页面截图等。
组件互通 6 分	**东西向接口：**公开组件列表查询、公开组件信息查询是否互通； **南北向接口：**组件注册、组件注销、组件列表查询、组件信息查询是否互通； 每个接口互通计 1 分，无法互通计 0 分。本项最多计 6 分。	系统架构设计文档、组件互通详细设计文档、组件互通接口设计文档及代码样例、测试记录报告、异构平台互联互通合作协议及组件互通运行信息，不限于运行日志、页面截图等。
流程互通 9 分	**东西向接口：**流程审批、流程审批确认、流程审批解除、审批状态查询是否互通； **南北向接口：**流程创建、流程更新、流程列表查询、流程信息查询、流程删除是否互通； 每个接口互通计 1 分，无法互通计 0 分。本项最多计 9 分。	系统架构设计文档、流程互通详细设计文档、流程互通接口设计文档及代码样例、测试记录报告、异构平台互联互通合作协议及流程互通运行信息，不限于运行日志、页面截图等。
任务互通 11 分	**东西向接口：**任务审批、任务审批确认、任务审批解除、审批状态查询是否互通； **南北向接口：**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、任务信息查询是否互通； 每个接口互通计 1 分，无法互通计 0 分。本项最多计 11 分。	系统架构设计文档、任务互通详细设计文档、任务互通接口设计文档及代码样例、测试记录报告、异构平台互联互通合作协议及任务互通运行信息，不限于运行日志、页面截图等。
模型互通 6 分	**东西向接口：**合作模型审批、合作模型审批确认、合作模型审批解除、合作模型审批查询是否互通； **南北向接口：**模型列表查询、模型信息查询	系统架构设计文档、模型互通详细设计文档、模型互通接口设计文档及代码样例、测试记录报告、异构平台互联互通合作协议及模型互通

指标分类及分值	评价要点	证明材料
	是否互通； 每个接口互通计 1 分，无法互通计 0 分。本项最多计 6 分。	运行信息，不限于运行日志、页面截图等。
数据安全性 20 分	**数据隐私保护**：是否基于隐私计算技术实现互联互通；原始数据是否出域；任意一方是否可基于运算结果反推出其它合作方原始数据。全部满足计 20 分，否则计 0 分。	系统架构设计文档、使用隐私计算算法协议清单及各算法安全报告文件，不限于算法实现原理、通信抓包数据及序列化数据、运行日志等。
结果正确性 20 分	**计算结果正确性**：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是否一致，或偏差在正常范围内。结果一致或偏差在正常范围内计 20 分，否则计 0 分。	提供计算样例数据、明文计算结果数据，以及基于多方安全计算平台计算结果数据。

12 评价等级

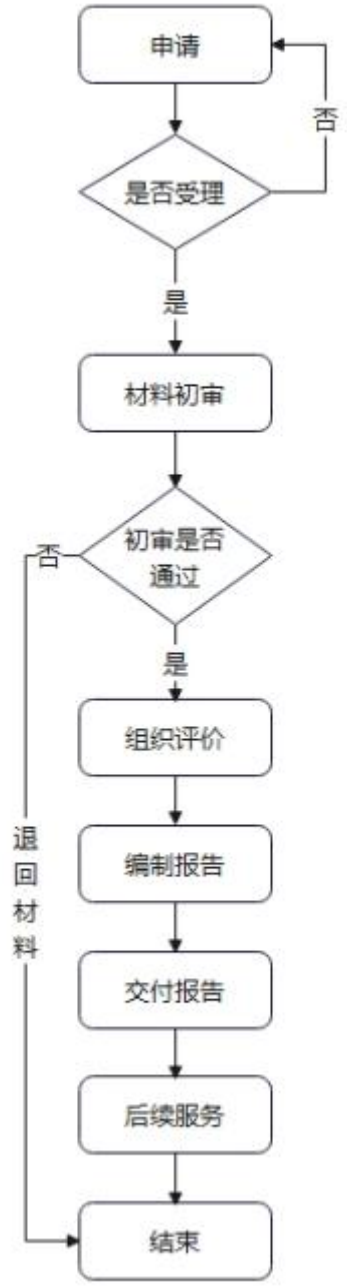
评价等级由低到高主要分为入门级、良好级、优秀级、卓越级四个等级，等级越高说明互联互通能力表现越优异。等级详情如表2所示。

表 2 多方安全计算互联互通评价等级

序号	指标内容	指标得分	评价等级	等级说明
1	结果正确性、数据安全性、节点互通、任务互通	[0,60)	-	平台不具备互联互通能力。
2		60	入门级	具备最基础互联互通能力。
3	结果正确性、数据安全性、节点互通、任务互通、项目互通、数据集互通、流程互通、组件互通、模型互通	(60,80]	良好级	具备良好的互联互通能力，能够实现一般的数据共享和基本的 API 调用，满足企业间少数业务场景。
4		(80,90]	优秀级	实现大部分的互联互通规范接口，具备良好的互联互通能力，可以满足企业间常见的业务场景。
5		(90,100]	卓越级	全面实现异构平台互联互通接口，具备卓越的互联互通能力，适合大型企业和跨行业合作，能够满足多方数据共享和协作的需求。

附　录　A （规范性）
多方安全计算互联互通应用评价流程

多方安全计算互联互通评价流程见图A.1。



图A.1 多方安全计算互联互通评价流程

附 录 B
（规范性）
多方安全计算互联互通应用评价报告模板

B.1 报告概述

B.1.1 背景

简要介绍多方安全计算的定义和应用场景，说明进行本次评价的目的与重要性。

B.1.2 评价对象

描述被评价的多方安全计算平台信息，包括其技术架构、主要功能和特性。

B.1.3 评价范围

明确本次评价的具体范围和具体指标。

B.2 评价方式

明确本次评价采取的具体方式。

B.3 评价方法

明确本次评价采取的具体评价方法。

B.4 评价结果

明确本次评价各指标的评价结果。

B.5 评价等级

明确本次评价的等级情况。

B.6 结论与建议

B.6.1 结论

基于评价结果，给出总体结论。

B.6.2 改进建议

提出针对发现问题的具体改进建议。

B.7 附录

附录A：评价指标说明
附录B：专家评审名单
附录C：数据收集方法和结果
附录D：参考文献

参 考 文 献