ICS 35.240.40
CCS A 11

团　　体　　标　　准

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

Privacy protection computing platform in financial scenario

—Technical requirements and test methods

2022－08－05 发布　　2022－11－05 实施

中国互联网协会　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。

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这些专利的责任。

本文件由中国互联网协会提出并归口。

本文件主要起草单位：中国信息通信研究院、中移动信息技术有限公司、联通数字科技有限公司、天翼电子商务有限公司、中国工商银行股份有限公司、成方金融科技有限公司、建信金融科技有限责任公司、腾讯云计算（北京）有限责任公司、阿里巴巴（中国）有限公司、蚂蚁科技集团股份有限公司、百度在线网络技术（北京）有限公司、小米数字科技有限公司、北京数牍科技有限公司、北京融数联智科技有限公司、上海富数科技有限公司、上海阵方科技有限公司、华控清交信息科技（北京）有限公司、上海同态信息科技有限责任公司、光之树(北京)科技有限公司

本文件主要起草人：郑威、张学阳、杨少杰、王榕、姜鼎、郭飞、梁心茹、茹志强、张帆、李大中、靳淑娴、周永明、贺伟、史楠迪、徐潜、强锋、相妹、柯琪锐、陆阳、涂锟、王雪、李武璐、霍昱光、昌文婷、袁鹏程、赵原、白晓媛、刘站奇、周斌、李克鹏、廖源、唐佳伟、季石磊、路卫杰、金银玉、单进勇、蔡超超、薛瑞东、陈剑、傅跃兵、卞阳、黄翠婷、龚自洪、沈敏文、王云河、靳晨、庞皓天、李朋林、钱佳威、沈敏均

金融场景隐私保护计算平台 技术要求与测试方法

1 范围

本文件规定了隐私保护计算平台应用于金融领域的安全性、性能和功能等技术要求内容，并给出了技术要求对应的测试方法。

本文件适用于银行、证券、保险等金融机构及相关合作机构隐私保护计算平台的设计、开发、测试和评估，也适用于第三方机构对金融场景隐私保护计算平台开展的检查、测试和评估工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 25069—2010 信息安全技术 术语

GB/T 28447—2012 信息安全技术 电子认证服务机构运营管理规范

GB/T 35295—2017 信息技术 大数据 术语

JR/T 0196—2020 多方安全计算金融应用技术规范

JR/T 0218—2021 金融业数据能力建设指引

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

在提供隐私保护的前提下，实现数据价值挖掘的技术体系，涉及联邦学习、多方安全计算、差分隐私、同态加密等技术。

3.2

联邦学习 federated learning

由两个或以上参与方共同参与，在保证数据方各自原始数据不出其定义的安全控制范围的前提下，协作构建并使用机器学习模型的技术架构。

[来源：IEEE P3652.1,有修改]

3.3

多方安全计算 secure multi-party computation

一组互不信任的参与方各自持有秘密数据，协同计算一个既定函数的问题，在保证参与方获得正确计算结果的同时，无法获得计算结果之外的任何信息。

[来源：JR/T 0196—2020，3.1,有修改]

3.4

差分隐私 differential privacy

一种通过加入随机噪声，最大化数据查询准确性，同时最大限度减少识别其记录机会的隐私保护算法。

3.5

同态加密 homomorphic encryption

一种满足明文空间到密文空间同态性的公钥加密算法。

3.6

数据集 data set

数据记录汇集的数据形式。
[来源：GB/T 35295—2017,2.1.46]

3.7

隐私信息检索 private information retrieval

客户端从数据库检索信息的一种方法，能够在保障客户端隐私安全的前提下，提供相应的检索服务。

3.8

超参数 hyperparameter

机器学习模型在开始学习过程之前设置的一个或多个参数。

3.9

计算因子 computation factor

基于多方安全计算输入数据产生的数据。
[来源：JR/T 0196—2020，3.3]

3.10

合作节点 coperative nodes

隐私保护计算合作方执行计算协议或算法逻辑的软件、计算机、虚拟计算机或集群。

3.11

客户画像 customer profile

各参与方通过安全共享数据抽象出某用户的信息全貌，临摹出该用户的行为习惯、消费习惯等重要信息。

3.12

可信执行环境 trusted execution environment

针对开放系统、基于芯片级隔离与安全引导、用于保证程序执行安全与数据存储真实性、完整性、机密性目标构建的一种软件运行环境。其中，芯片级隔离是指基于主芯片安全扩展机制通过对计算资源的固定划分或动态共享，保证所隔离资源不被开放系统访问的一种安全机制。

3.13

金融场景 financial scenario

一种数据流通共享和协同应用的业务场景，该业务场景中使用了金融数据，或者产出了可以直接或间接应用于金融行业的产品服务。

4 缩略语

下列缩略语适用于本文件：

AUC	ROC曲线下的面积	Area Under Curve
DNN	深度神经网络	Deep Neural Networks
IV	信息价值	Information Value
K-Means	K均值聚类算法	K-Means Clustering Algorithm
KS	洛伦兹曲线	Kolmogorov-Smirnov Curve
MSE	均方误差	Mean Square Error
WOE	证据权重	Weight of Evidence
XGBoost	极致梯度提升	eXtreme Gradient Boosting

5 参考架构

5.1 联邦学习参考架构

在联邦学习架构中，参与方主要承担的角色有协调方、数据方、计算方和结果方，参考架构如图 1所示。协调方是协调各参与方协作构建联邦模型的参与方，协调方宜取得其它参与方的信任或由具备公信力的第三方机构担任，作为非必要角色，协调方有可能不存在于联邦学习架构中；数据方是指提供联邦模型建模所需的私有数据的参与方；计算方是指执行联邦学习计算的参与方；结果方是指获取联邦学习结果的参与方。一个联邦学习参与方可承担多个角色。在联邦学习架构实际部署中，数据方和协调方通常会同时承担计算方的角色。

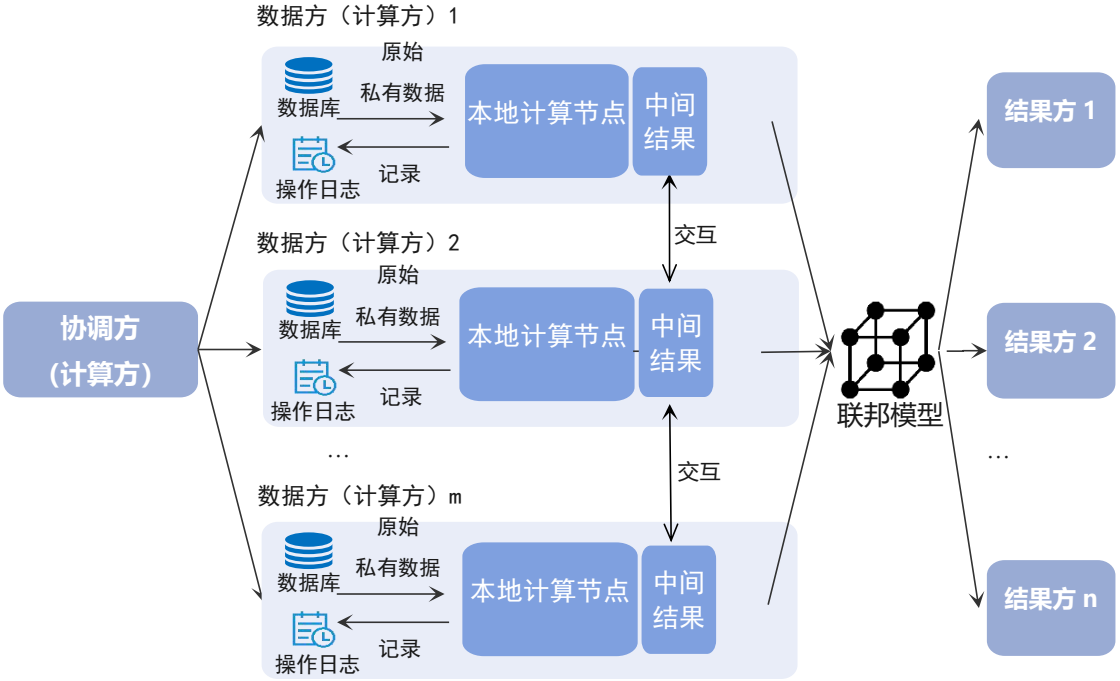

图 1　联邦学习参考架构

5.2 多方安全计算参考架构

在多方安全计算架构中，参与方主要承担的角色包括任务发起方、数据方、算法方、调度方、计算方和结果方。任务发起方负责核实任务的资源到位情况并发起任务；数据方为多方安全计算任务提供原始输入数据；算法方提供用以计算的算法，算法可由单独的一方提供，也可由数据方或计算方提供；调度方负责对所有任务进行综合调度；计算方提供多方安全计算协议的算力，负责多方安全计算任务的实际执行；结果方指多方安全计算结果的接收方。多方安全计算参考架构如图 2所示。在一次多方安全计算任务中，数据方将输入数据转化为输入计算因子并发送给计算方，计算方接收数据方发送的计算因子，按照多方安全计算协议进行协同计算，并将结果计算因子发送给结果方。在多方安全计算任务的执行过程中，一个参与方可以同时承担多个角色。

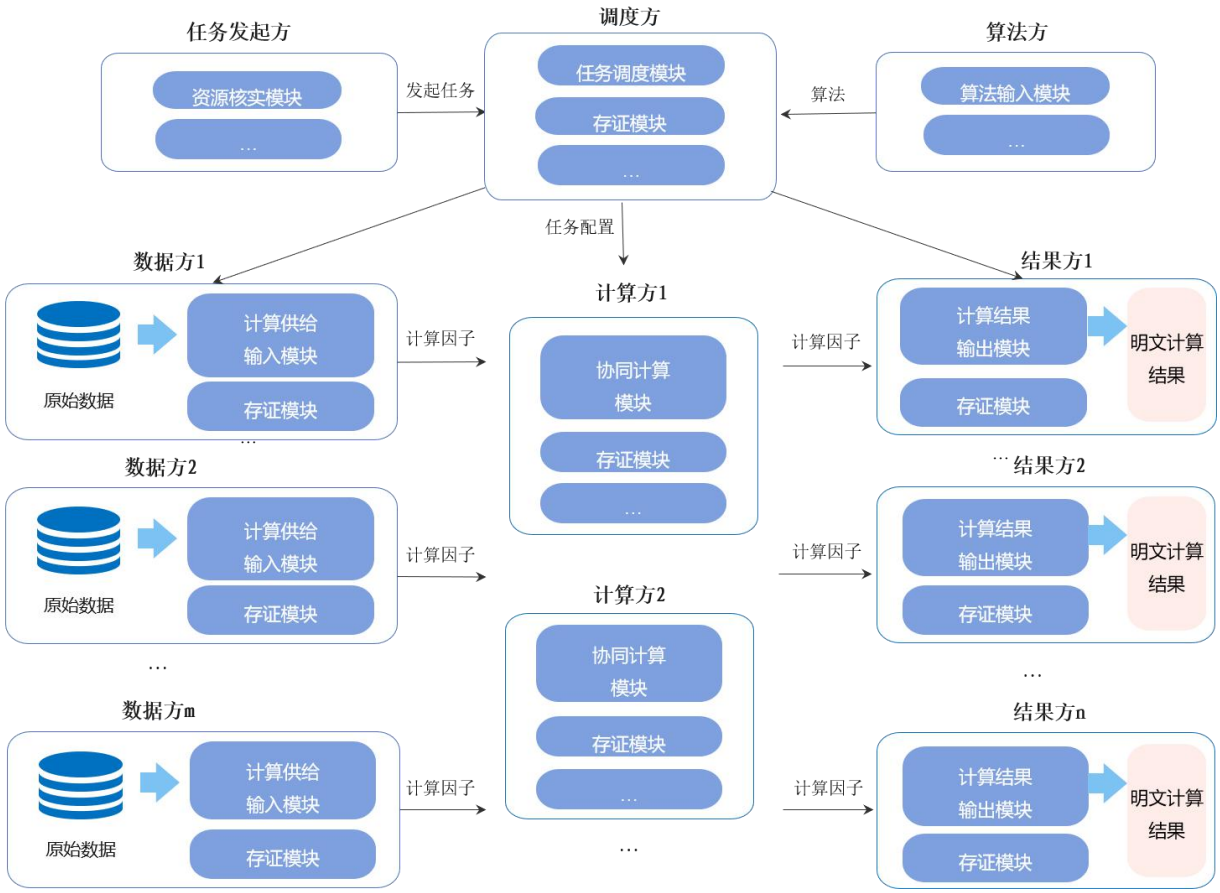

图 2　多方安全计算参考架构

5.3 可信执行环境参考架构

在可信执行环境架构中，参与方主要承担的角色包括数据方、计算方和结果方。数据方是指可信执行环境架构中提供原始数据的参与方，通常由存证模块、数据处理和加密模块、认证模块和数据组成；计算方是指提供计算平台的参与方，计算平台通常由存证模块、认证模块、数据加解密模块、计算模块组成，基于可信硬件的可信执行环境通常部署在计算方；结果方是指获取最终计算结果的参与方，通常由存证模块、解密模块组成。其中，数据方的数据在进行处理后，通过加密密钥进行加密，再上传到计算方的可信计算环境中，计算方通过解密密钥对加密数据进行解密后，发送给计算模块，对解密后的多方数据进行相关计算，计算结果加密后发送给结果方，确保隐私信息不会泄露，整个过程中存证模块可通过日志、区块链等对数据使用等关键信息进行记录，便于审计和追溯。可信执行环境参考架构图 3所示。

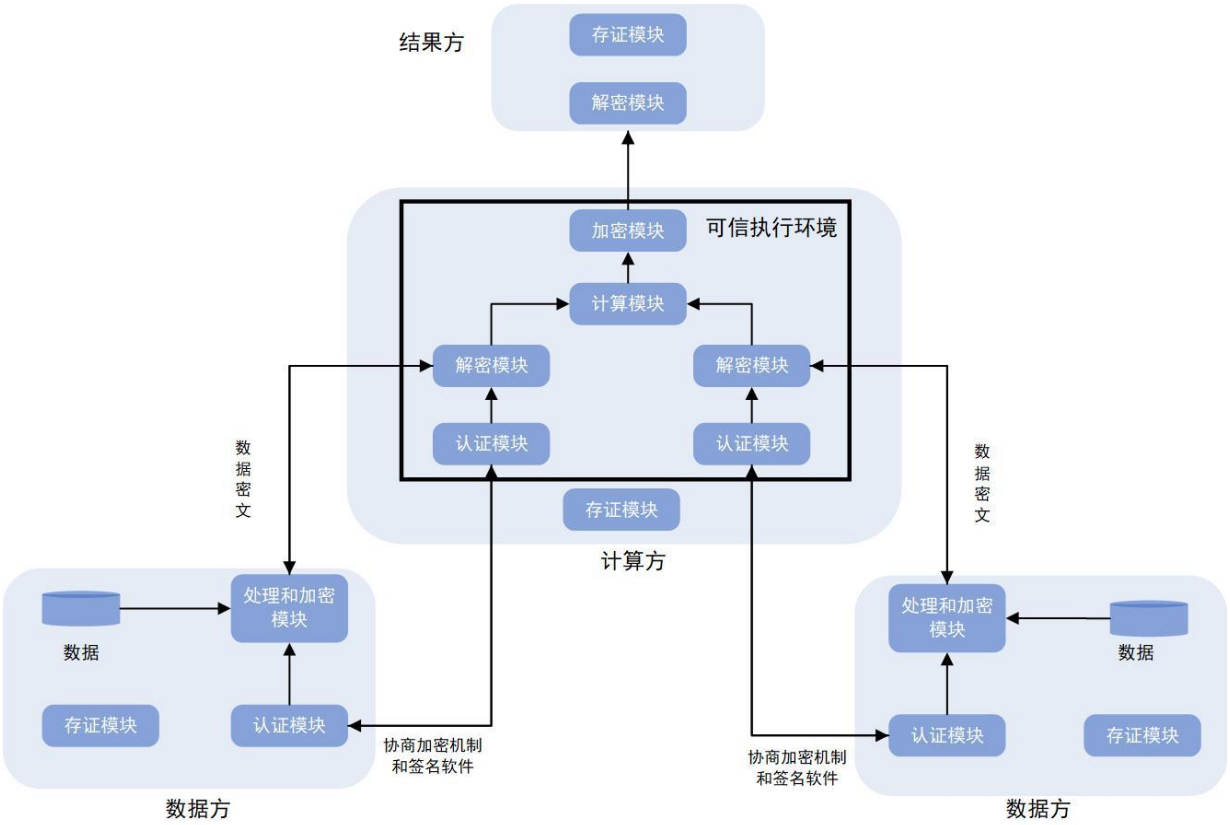

图 3　可信执行环境参考架构

6　技术要求

6.1 概述

金融场景隐私保护计算平台的主要能力是在保障数据安全的前提下实现金融数据的共享、流通和协同应用。本文件主要从隐私保护计算能力、金融场景应用能力、原理架构安全能力、平台管理能力等维度对相关产品或平台提出技术要求。技术要求总结如表 1，具体要求见后续章节。

表 1　金融场景隐私保护计算平台技术要求总结

技术要求	具体要求
隐私保护计算能力	隐私匹配查询能力（4 个测试用例）
	基础多方运算能力（3 个测试用例）
	联合特征工程能力（4 个测试用例）
	多方联合建模能力（6 个测试用例）
	模型评估能力（1 个测试用例）

	多方联合预测能力（12 个测试用例）
金融场景应用能力	金融风控场景（1 个测试场景）
	客户画像场景（1 个测试场景）
	多方黑名单查询场景（1 个测试场景）
	反洗钱场景（1 个测试场景）
	精准营销场景（1 个测试场景）
	普惠金融场景（1 个测试场景）
原理架构安全能力	匿名匹配/查询安全性（1 个测试用例）
	基础多方运算安全性（1 个测试用例）
	多方联合建模安全性（1 个测试用例）
	多方联合预测安全性（1 个测试用例）
	计算架构安全性（1 个测试用例）
平台管理能力	用户管理能力（1 个测试用例）
	节点管理能力（1 个测试用例）
	接口安全防护能力（1 个测试用例）
	数据管理能力（1 个测试用例）
	数据库支持能力（1 个测试用例）
	任务管理能力（1 个测试用例）
	系统日志审计能力（1 个测试用例）
	系统监控告警能力（1 个测试用例）
	网络容错能力（1 个测试用例）
	多数据方计算能力（1 个测试用例）

6.2 隐私保护计算能力

6.2.1 隐私匹配查询能力

金融场景隐私保护计算平台应支持隐私求交匹配、隐私信息检索能力，包括海量数据离线隐私匹配检索和在线隐私匹配检索，性能应满足金融实际业务要求。

6.2.2 基础多方运算能力

金融场景隐私保护计算平台应支持基础的多方运算能力，包括多方加减乘除、比较和统计等，性能应满足金融实际业务要求。

6.2.3 联合特征工程能力

金融场景隐私保护计算平台应具备准确的多方数据预处理能力。包括但不限于数据清洗、特征转换、特征筛选、数据分箱等，性能应满足金融实际业务要求。

6.2.4 多方联合建模能力

金融场景隐私保护计算平台应支持常见机器学习模型的多方联合建模，建模性能应满足金融实际业务要求。

6.2.5 模型评估能力

金融场景隐私保护计算平台应具备机器学习模型评估能力，包括但不限于回归模型的 MSE，分类模型的 AUC 值、KS 值等评估指标功能。

6.2.6 多方联合预测能力

金融场景隐私保护计算平台应支持常见机器学习模型的多方联合预测，预测性能应满足金融实际业务要求。

6.3 金融场景应用能力

6.3.1 金融风控场景

金融场景隐私保护计算平台应具备在金融风控场景的实际落地能力，包括匿名数据的关联、数据的预处理、联合风控模型的建立和调用等功能。

6.3.2 客户画像场景

金融场景隐私保护计算平台应具备在用户群体画像场景的实际落地能力，支持多方联合临摹特定用户群体画像等功能。

6.3.3 多方黑名单查询场景

金融场景隐私保护计算平台应具备在黑名单查询场景的实际落地能力，支持多方黑名单的匿名联合查询，包括离线查询和在线查询等。

6.3.4 反洗钱场景

金融场景隐私保护计算平台应具备在反洗钱场景的实际落地能力，包括匿名数据的关联、数据的预处理、联合反洗钱模型的建立和调用等功能。

6.3.5 精准营销场景

金融场景隐私保护计算平台应具备在精准营销场景的实际落地能力，包括匿名数据的关联、数据的预处理、联合精准营销模型的建立和调用等功能。

6.3.6 普惠金融场景

金融场景的隐私保护计算平台宜具备在普惠金融服务场景的实际落地能力，包括匿名数据的关联、数据的预处理、普惠金融模型的建立和调用等功能。

6.4 原理架构安全能力

6.4.1 匿名匹配/查询安全性

匿名匹配/查询功能安全性应符合 JR/T 0196—2020 相关安全要求，应保证安全原理与系统代码、运行日志、通信数据的一致性。系统使用的算法宜考虑算法透明度、算法公平性问题。系统使用的相关密码技术，其选型、密钥长度、密钥管理方式等，宜按照相应国家标准进行设计与实施。

6.4.2 基础多方运算安全性

基础多方运算安全性应符合 JR/T 0196—2020 相关安全要求，应保证安全原理与系统代码、运行日志、通信数据的一致性。系统使用的算法宜考虑算法透明度、算法公平性问题。系统使用的相关密码技术，其选型、密钥长度、密钥管理方式等，宜按照相应国家标准进行设计与实施。

6.4.3 多方联合建模安全性

多方联合建模安全性宜符合 JR/T 0196—2020 相关安全要求，应保证安全原理与系统代码、运行日志、通信数据的一致性。系统使用的算法宜考虑算法透明度、算法公平性问题。系统使用的相关密码技术，其选型、密钥长度、密钥管理方式等，宜按照相应国家标准进行设计与实施。

6.4.4 多方联合预测安全性

多方联合预测安全性宜符合 JR/T 0196—2020 相关安全要求，应保证安全原理与系统代码、运行日志、通信数据的一致性。系统使用的算法宜考虑算法透明度、算法公平性问题。系统使用的相关密码技术，其选型、密钥长度、密钥管理方式等，宜按照相应国家标准进行设计与实施。

6.4.5 计算架构安全性

平台架构安全性宜符合 JR/T 0196—2020 相关安全要求，应保证安全原理与系统代码、运行日志、通信数据的一致性。系统使用的算法宜考虑算法透明度、算法公平性问题。系统使用的相关密码技术，其选型、密钥长度、密钥管理方式等，宜按照相应国家标准进行设计与实施。

6.5 平台管理能力

6.5.1 用户管理能力

金融场景隐私保护计算平台应具备对于用户的身份认证能力，认证方式包括但不限于口令认证、证书认证、令牌认证等。应支持用户的权限管理，阻止用户的非法越权操作。

6.5.2 节点管理能力

金融场景隐私保护计算平台应支持节点管理能力，包括但不限于节点身份认证、合作节点新增、删除和上下线，应保证仅能与通过认证的合作节点开展正常工作。

6.5.3 接口安全防护能力

金融场景隐私保护计算平台应具备对外公开接口的安全限制和安全控制措施，包括但不限于接口访问和调用的身份鉴别、设备鉴权、访问控制和审计机制等。

6.5.4 数据管理能力

金融场景隐私保护计算平台应支持数据管理能力，包括但不限于数据的导入、增加、查看、删除、以及相关权限的控制。

6.5.5 数据库支持能力

金融场景隐私保护计算平台应支持常见数据库的使用，能正确的将外部数据导入并顺利参与计算。

6.5.6 任务管理能力

金融场景隐私保护计算平台应支持任务管理相关能力，包括但不限于任务的创建、任务调度、状态监控和多任务并行等。

6.5.7 系统日志审计能力

金融场景隐私保护平台应具备系统日志和审计相关能力，能够通过日志、区块链等对用户操作、数据使用等关键信息进行存证记录，便于审计和追溯。相关能力应符合 JR/T 0218—2021 中 11.3 规定的数据保护审计相关工作措施要求。

6.5.8 系统监控告警能力

金融场景隐私保护计算平台应支持系统监控告警能力，应能够持续监控系统运行状态，支持对系统异常状态的快速识别和响应。

6.5.9 网络容错能力

金融场景隐私保护计算平台应具备一定的容错能力，平台应具备在复杂网络环境中保持稳定运行的能力，应容忍网络震荡并快速恢复运行状态。

6.5.10 多数据方计算能力

金融场景的隐私保护计算平台宜支持超过两个数据方的多方计算、联合建模和联合预测等能力。

7 测试方法

7.1 概述

依据前一章提出的金融场景隐私保护计算平台技术要求，本文件对金融场景隐私保护计算平台的测试方法进行了详细描述，为每个测试用例提供了测试用表。测试用表具体构成项何含义如表 2。

表 2 测试用表构成项和含义

构成项	含义
用例编号	本文件中对于测试用例的编号，由字母和数字组成，首位为字母。四个维度测试用

	例首字母不同，隐私保护计算能力用例首字母为A，金融场景应用能力用例首字母为F，原理架构安全能力用例首字母为S，平台管理能力用例首字母为S。
用例分类	用例归属的能力分类。
验证目的	用例测试的主要内容。
预置条件	开展用例测试前需要准备好的事项。
验证步骤	用例实际测试步骤。
预期结果	执行用例应输出的结果。
实际结果	实际执行用例输出的结果。
备注	用例测试中其他需要说明的问题。

7.2 隐私保护计算能力

7.2.1 隐私匹配查询能力

7.2.1.1 离线隐私求交/匹配

用例编号：A101	
用例分类：隐私匹配查询能力	
验证目的：验证系统具备离线求交匹配功能。该功能是一项基础功能，是后续操作的先决条件。离线测试没有实时要求，主要测试海量数据的处理能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行匿名求交匹配任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确求交结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 匹配错误率
备注:	

7.2.1.2 实时匿名匹配

用例编号：A102
用例分类：隐私匹配查询能力

验证目的：验证系统具备实时在线匿名匹配能力，例如黑名单匹配查询。实时环境主要应对实时场景，测试重点为延时性。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行在线匿名匹配任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确求交结果。	
测试结果	1. A 方输入数据（截图需包含数据量和 ID 值） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 单次任务执行时间 单次任务网络传输量 匹配错误率
备注：	

7.2.1.3 离线隐私信息检索

用例编号：A103	
用例分类：隐私匹配查询能力	
验证目的：验证系统具备隐私信息检索能力。该功能是一项基础功能，离线测试没有实时要求，主要测试海量数据的处理能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行隐私信息检索任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确检索结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 检索错误率
备注：	

7.2.1.4 实时隐私信息检索

用例编号：A104	
用例分类：隐私匹配查询能力	
验证目的：验证系统具备实时隐私信息检索能力。实时环境主要应对实时场景，测试重点为延时性。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行在线隐私信息检索任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确检索结果。	
测试结果	1. A 方输入数据（截图需包含数据量和 ID 值） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 单次任务执行时间 单次任务网络传输量 检索错误率
备注：	

7.2.2 基础多方运算能力

7.2.2.1 加减乘除算法

用例编号：A201
用例分类：基础多方运算能力
验证目的：验证系统是否支持加减乘除等基础多方运算能力。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。
验证步骤： 1. 执行多方计算功能，基于双方数据计算每个样本的加减乘除计算任务。
预期结果： 1. 任务正常执行，性能达到应用需求，并且每一行都输出正确计算结果。

测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果（四个计算结果需单独呈现） 任务执行时间 网络传输量 计算精度
备注：	

7.2.2.2 比较运算

用例编号：A202	
用例分类：基础多方运算能力	
验证目的：验证系统是否支持比较计算能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行多方计算功能，比较每个样本在双方间谁更大、或者相同。	
预期结果： 1. 任务正常执行，性能达到应用需求，能输出正确计算结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 计算精度
备注：	

7.2.2.3 基础统计运算

用例编号：A203
用例分类：基础多方运算能力
验证目的：验证系统是否支持基础统计运算。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。

验证步骤： 1. 执行多方计算功能，计算全体样本的统计数据，包括和、平均值、方差、最值和分位值。	
预期结果： 1. 任务正常执行，性能达到应用需求，。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果（三个计算结果需单独呈现） 任务执行时间 网络传输量 计算精度
备注：	

7.2.3 联合特征工程能力

7.2.3.1 数据清洗

用例编号：A301	
用例分类：联合特征工程能力	
验证目的：验证系统具有数据清洗的功能	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 正确完成数据清洗任务，包括缺失值处理、异常值处理等。	
预期结果： 1. 能够正确完成相关数据清洗任务。	
测试结果	1. A 方输入数据（截图需包含缺失数据或异常值） 2. B 方输入数据（截图需包含缺失数据或异常值） 3. 任务配置信息 4. A 方输出数据（截图需包含处理过的缺失数据或异常值） 5. B 方输出数据（截图需包含处理过的缺失数据或异常值）
备注：	

7.2.3.2 特征转换

用例编号：A302
用例分类：联合特征工程能力
验证目的：验证系统具有特征转换的功能。
预置条件：

1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 完成特征转换任务，包括独热编码（one-hot encoding）、WOE、归一化等。	
预期结果： 1. 正确完成特征转换任务，包括独热编码（one-hot encoding）、WOE、归一化等。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. A 方输出数据（截图需包含处理过的新数值） 5. B 方输出数据（截图需包含处理过的新数值）
备注：	

7.2.3.3 特征筛选

用例编号：A303	
用例分类：联合特征工程能力	
验证目的：验证系统具有安全的特征筛选功能。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行特征筛选任务，包括常见的 IV 值、相关性等。	
预期结果： 1. 支持特征筛选的常见方法，如 IV 值、相关性等。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. 基于双方数据的 IV 值、相关性结果或报告。
备注：	

7.2.3.4 分箱

用例编号：A304
用例分类：联合特征工程能力
验证目的：支持常见的分箱功能，如等频分箱、等距分箱等。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。

3. 双方模拟真实场景准备数据。	
验证步骤： 1. 对虚拟融合的数据集进行特征分箱处理，包括等频分箱、等距分箱等。	
预期结果： 1. 正确执行分箱任务。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. A 方基于不同分箱的输出数据 5. B 方基于不同分箱的输出数据
备注：	

7.2.4 多方联合建模能力

7.2.4.1 有监督学习

7.2.4.1.1 线性回归模型训练

用例编号：A401	
用例分类：多方联合建模能力	
验证目的：验证支持实际生产数据量级别的线性回归模型训练。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 将数据分为训练集和测试集。 2. 以训练数据集为基础创建线性回归模型训练。 3. 以测试数据集为基础衡量模型训练结果。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确建模结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 MSE
备注：	

7.2.4.1.2 逻辑回归模型训练

用例编号：A402

用例分类：多方联合建模能力	
验证目的：验证支持实际生产数据量级别的逻辑回归模型训练。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 将数据分为训练集和测试集。 2. 以训练数据集为基础创建逻辑回归模型训练。 3. 以测试数据集为基础衡量模型训练结果。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确建模结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 AUC
备注：	

7.2.4.1.3 XGBoost 模型训练

用例编号：A403	
用例分类：多方联合建模能力	
验证目的：验证支持实际生产数据量级别的 XGBoost 模型训练	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 设置超参数。 2. 将数据分为训练集和测试集。 3. 以训练数据集为基础创建 XGBoost 模型训练。 4. 以测试数据集为基础衡量模型训练结果。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确建模结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量

	AUC
备注：	

7.2.4.1.4 DNN 模型训练

用例编号：A404	
用例分类：多方联合建模能力	
验证目的：验证支持实际生产数据量级别的 DNN 模型训练	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 设置超参数。 2. 将数据分为训练集和测试集。 3. 以训练数据集为基础创建 DNN 模型训练。 4. 以测试数据集为基础衡量模型训练结果。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确建模结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 AUC
备注：	

7.2.4.2 无监督学习

7.2.4.2.1 K-Means 模型训练

用例编号：A405
用例分类：多方联合建模能力
验证目的：验证支持实际生产数据量级别的 K-Means 模型训练。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。
验证步骤： 1. 将数据分为训练集和测试集。

2. 以训练数据集为基础创建 K-Means 模型训练。 3. 以测试数据集为基础衡量模型训练结果。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确建模结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果
备注：	

7.2.4.3 其它学习

7.2.4.3.1 迁移学习

用例编号：A406	
用例分类：多方联合建模能力	
验证目的：验证支持实际生产数据量级别的迁移学习模型训练。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 将数据分为训练集和测试集。 2. 以训练数据集为基础创建迁移学习模型训练。 3. 以测试数据集为基础衡量模型训练结果。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确建模结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果
备注：	

7.2.5 模型评估能力

用例编号：A501
用例分类：模型评估能力
验证目的：验证支持联合建模的模型评估，如回归模型的 MSE，分类模型的 AUC 值、KS 值等统计指标。
预置条件： 1. A、B 双方系统部署完成。

2. 登录账户。 3. 针对不同的模型训练算法，模拟真实场景准备数据。	
验证步骤： 1. 创建模型评估任务。	
预期结果： 1. 任务正常执行，并输出正确的模型评估值。	
测试结果	1. 任务配置信息 2. 模型评价结果或报告
备注：	

7.2.6 多方联合预测能力

7.2.6.1 有监督学习预测

7.2.6.1.1 线性回归模型离线预测

用例编号：A601	
用例分类：多方联合预测能力	
验证目的：验证系统具有离线安全调用线性回归模型功能，测试重点为海量数据。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行线性回归模型离线调用。 2. 双方模拟真实场景准备数据。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 MSE（根据真实标签计算）
备注：	

7.2.6.1.2 线性回归模型实时预测

用例编号：A602

用例分类：多方联合预测能力	
验证目的：验证系统具有实时安全调用线性回归模型功能，测试重点为实时能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行在线预测任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. 输出结果 单次任务执行时间 单次任务网络传输量 MSE（根据真实标签计算）
备注：	

7.2.6.1.3 逻辑回归模型离线预测

用例编号：A603	
用例分类：多方联合预测能力	
验证目的：验证系统具有离线安全调用逻辑回归模型功能，测试重点为海量数据。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行逻辑回归模型离线调用。 2. 双方模拟真实场景准备数据。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 AUC（根据真实标签计算）
备注：	

7.2.6.1.4 逻辑回归模型实时预测

用例编号：A604	
用例分类：多方联合预测能力	
验证目的：验证系统具有实时安全调用逻辑回归模型功能，测试重点为实时能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行在线预测任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. 输出结果 单次任务执行时间 单次任务网络传输量 AUC（根据真实标签计算）
备注：	

7.2.6.1.5 XGBoost 模型离线预测

用例编号：A605	
用例分类：多方联合预测能力	
验证目的：验证系统具有离线安全调用 XGBoost 模型功能，测试重点为海量数据。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行 XGBoost 模型离线调用。 2. 双方模拟真实场景准备数据。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果 任务执行时间 网络传输量 AUC（根据真实标签计算）

备注：

7.2.6.1.6 XGBoost 模型实时预测

用例编号：A606	
用例分类：多方联合预测能力	
验证目的：验证系统具有实时安全调用 XGBoost 模型功能，测试重点为实时能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行在线预测任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. 输出结果 单次任务执行时间 单次任务网络传输量 AUC（根据真实标签计算）
备注：	

7.2.6.1.7 DNN 模型离线预测

用例编号：A607	
用例分类：多方联合预测能力	
验证目的：验证系统具有离线安全调用 DNN 模型功能，测试重点为海量数据。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行 DNN 模型离线调用。 2. 双方模拟真实场景准备数据。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果

果	任务执行时间 网络传输量 AUC（根据真实标签计算）
备注：	

7.2.6.1.8 DNN 模型实时预测

用例编号：A608	
用例分类：多方联合预测能力	
验证目的：验证系统具有实时安全调用 DNN 模型功能，测试重点为实时能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行在线预测任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. 输出结果 单次任务执行时间 单次任务网络传输量 AUC（根据真实标签计算）
备注：	

7.2.6.2 无监督学习预测

7.2.6.2.1 K-Means 模型离线预测

用例编号：A609
用例分类：多方联合预测能力
验证目的：验证系统具有离线安全调用 K-means 模型功能，测试重点为海量数据。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。
验证步骤： 1. 根据训练完成的模型，执行 K-Means 模型离线调用。 2. 双方模拟真实场景准备数据。

预期结果： 2. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果
备注：	

7.2.6.2.2 K-Means 模型实时预测

用例编号：A610	
用例分类：多方联合预测能力	
验证目的：验证系统具有实时安全调用 K-Means 模型功能，测试重点为实时能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行在线预测任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. 输出结果
备注：	

7.2.6.3 其它学习预测

7.2.6.3.1 迁移学习离线预测

用例编号：A611
用例分类：多方联合预测能力
验证目的：验证系统具有离线安全调用迁移学习模型功能，测试重点为海量数据。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。
验证步骤： 1. 根据训练完成的模型，执行迁移学习模型离线调用。

2. 双方模拟真实场景准备数据。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. 任务配置信息 4. 输出结果
备注：	

7.2.6.3.2 迁移学习实时预测

用例编号：A612	
用例分类：多方联合预测能力	
验证目的：验证系统具有实时安全调用迁移学习模型功能，测试重点为实时能力。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 根据多方联合建模部分训练任务，已经完成对应模型训练。	
验证步骤： 1. 根据训练完成的模型，执行在线预测任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确预测结果。	
测试结果	1. A 方输入数据 2. B 方输入数据 3. 任务配置信息 4. 输出结果
备注：	

7.3 金融场景应用能力

7.3.1 金融风控场景

用例编号：F101
场景分类：金融场景应用能力
验证目的：验证系统具有在贷款风控场景的实际落地能力，包括样本的匿名数据关联，样本的预处理，联合风控模型的建立，联合风控模型的调用。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。

3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行匿名匹配/查询任务。 2. 执行特征工程任务，如数据清洗、特征转换、特征筛选、分箱等。 3. 执行联合风控建模（如评分卡模型、XGBoost 等）。 4. 执行模型预测任务（离线+实时）。	
预期结果： 1. 完整执行上述步骤。 2. 各个任务正常执行，并输出正确预测结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. PSI 配置信息： 4. PSI 输出结果： 5. 特征工程配置信息 6. 特征工程输出结果 7. 建模配置信息 8. 建模运行结果 9. 离线预测运行结果 10. 实时预测运行结果
备注：	

7.3.2 客户画像场景

用例编号：F201	
场景分类：金融场景应用能力	
验证目的：验证系统具有用户群体的画像构建功能，具有获得相关画像特征的功能，构建特定用户群体的画像。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行匿名匹配/查询任务。 2. 进行多方联合统计分析，得到不同标签下样本在 B 方特征下的统计指标和分布（例如年龄，性别）。 3. 构建特定用户群体的画像。	
预期结果： 1. 完整执行上述步骤。 2. 能够计算相关的画像特征，达到实际应用需求。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. PSI 配置信息： 4. PSI 输出结果： 5. 画像统计配置信息 6. 画像统计运行结果

备注：

7.3.3 多方黑名单联合查询场景

用例编号：F301	
场景分类：金融场景应用能力	
验证目的：验证系统支持多方黑名单查询功能。包括离线查询和在线查询。	
预置条件： 1. 多方系统部署完成。 2. 登录账户。 3. 多方模拟真实场景准备数据。	
验证步骤： 1. 执行基于隐私匹配的黑名单查询任务。	
预期结果： 1. 任务正常执行，性能达到应用需求，并输出正确查询结果。	
测试结果	1. 各方输入数据（截图需包含数据量） 2. 各方查询配置信息 3. 各方按照隐私查询方案，完成联合查询任务，获取查询结果，检验查询结果是否正确
备注:	

7.3.4 反洗钱场景

用例编号：F401
场景分类：金融场景应用能力
验证目的：验证系统具有在反洗钱场景的实际落地能力，包括样本的匿名数据关联，样本的预处理，联合反洗钱模型的建立，联合反洗钱模型的调用。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。
验证步骤： 1. 执行匿名匹配/查询任务。 2. 执行特征工程任务，如数据清洗、特征转换、特征筛选、分箱等。 3. 执行反洗钱建模（如评分卡模型、XGBoost 等）。 4. 执行模型预测任务（离线+实时）。
预期结果： 1. 完整执行上述步骤。 2. 各个任务正常执行，并输出正确预测结果。

测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. PSI 配置信息： 4. PSI 输出结果： 5. 特征工程配置信息 6. 特征工程输出结果 7. 建模配置信息 8. 建模运行结果 9. 离线预测运行结果 10. 实时预测运行结果
备注：	

7.3.5 精准营销场景

用例编号：F501
场景分类：金融场景应用能力
验证目的：验证系统具有在精准营销场景的实际落地能力，包括样本的匿名数据关联，样本的预处理，联合精准营销模型的建立，联合精准营销模型的调用。
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。
验证步骤： 1. 执行匿名匹配/查询任务。 2. 执行特征工程任务，如数据清洗、特征转换、特征筛选、分箱等。 3. 执行精准营销建模（如评分卡模型、XGBoost 等）。 4. 执行模型预测任务（离线+实时）。
预期结果： 1. 完整执行上述步骤。 2. 各个任务正常执行，并输出正确预测结果。
测试结果： 1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. PSI 配置信息： 4. PSI 输出结果： 5. 特征工程配置信息 6. 特征工程输出结果 7. 建模配置信息 8. 建模运行结果 9. 离线预测运行结果 10. 实时预测运行结果
备注：

7.3.6 普惠金融场景

用例编号：F601

场景分类：金融场景应用能力	
验证目的：验证系统具有在普惠金融的实际落地能力，包括样本的匿名数据关联，样本的预处理，普惠金融模型的建立，联合普惠金融模型的调用。	
预置条件： 1. A、B 双方系统部署完成。 2. 登录账户。 3. 双方模拟真实场景准备数据。	
验证步骤： 1. 执行匿名匹配/查询任务。 2. 执行特征工程任务，如数据清洗、特征转换、特征筛选、分箱等。 3. 执行普惠金融建模（如评分卡模型、XGBoost 等）。 4. 执行模型预测任务（离线+实时）。	
预期结果： 1. 完整执行上述步骤。 2. 各个任务正常执行，并输出正确预测结果。	
测试结果	1. A 方输入数据（截图需包含数据量） 2. B 方输入数据（截图需包含数据量） 3. PSI 配置信息： 4. PSI 输出结果： 5. 特征工程配置信息 6. 特征工程输出结果 7. 建模配置信息 8. 建模运行结果 9. 离线预测运行结果 10. 实时预测运行结果
备注：	

7.4 原理架构安全能力

7.4.1 匿名匹配/查询安全性

用例编号：P101
用例分类：原理架构安全能力
验证目的：论证匿名匹配/查询具有架构上的算法安全性、代码一致性和运行一致性。
预置条件： 1. 提供匿名匹配/查询的设计、原理说明文档。 2. 提供匿名匹配/查询的安全性论证材料，包括采用的协议算法、密码技术、安全假设、安全性定义等相关论证材料。

3. 提供匿名匹配/查询的执行日志。 4. 提供部分相关代码。
预期结果： 1. 通过安全性论证，达到要求的计算安全级别，具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料。 2. 代码实现和相关文档、执行日志、通信数据是一致的。
备注：

7.4.2 基础多方运算安全性

用例编号：P201
用例分类：原理架构安全能力
验证目的：论证基础多方运算具有架构上的算法安全性、代码一致性和运行一致性。
预置条件： 1. 提供基础多方运算的设计、原理说明文档。 2. 提供基础多方运算的安全性论证材料，包括采用的协议算法、密码技术、安全假设、安全性定义等相关论证材料。 3. 提供基础多方运算的执行日志。 4. 提供部分相关代码。
预期结果： 1. 通过安全性论证，达到要求的计算安全级别，具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料。 2. 代码实现和相关文档、执行日志、通信数据是一致的。
备注：

7.4.3 多方联合建模安全性

用例编号：P301
用例分类：原理架构安全能力
验证目的：论证多方联合建模具有架构上的算法安全性、代码一致性和运行一致性。
预置条件： 1. 提供多方联合建模设计、原理说明文档。 2. 提供多方联合建模安全性论证材料，包括采用的协议算法、密码技术、安全假设、安全性定义等相关论证材料。 3. 提供多方联合建模的执行日志。 4. 提供部分相关代码。
预期结果： 1. 通过安全性论证，达到要求的计算安全级别，具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料。

2. 代码实现和相关文档、执行日志、通信数据是一致的。
备注：

7.4.4 多方联合预测安全性

用例编号：P401
用例分类：原理架构安全能力
验证目的：论证多方联合模型调用具有架构上的算法安全性、代码一致性和运行一致性。
预置条件： 1. 提供多方联合预测设计、原理说明文档。 2. 提供多方联合预测安全性论证材料，包括采用的协议算法、密码技术、安全假设、安全性定义等相关论证材料。 3. 提供多方联合预测的执行日志。 4. 提供部分相关代码。
预期结果： 1. 通过安全性论证，达到要求的计算安全级别，具备已发表的论文证明或由专家对协议安全进行评审并出具证明材料。 2. 代码实现和相关文档、执行日志是一致、通信数据的。
备注：

7.4.5 计算架构安全性

用例编号：P501
用例分类：原理架构安全能力
验证目的：论证隐私保护计算平台的架构类型，以及不同架构下的安全性水平。
预置条件： 1. 提供 7.4.1、7.4.2、7.4.3、7.4.4 的相关材料。 2. 通过 7.4.1、7.4.2、7.4.3、7.4.4 的安全性论证。
预期结果： 1. 通过上述安全性论证，能够明确判断系统的架构类型（如去中心化架构或有中心化架构），架构原理符合相应的安全性要求。
备注：

7.5 平台管理能力

7.5.1 用户管理能力

用例编号：S101
用例分类：平台管理能力

验证目的： 验证平台具备用户管理相关功能。
预置条件： 1. 完成系统的部署。 2. 登录管理员账户。
验证步骤： 1. 新建普通用户，并选择用户的权限范围。 2. 使用错误的口令、证书或令牌登录普通用户； 3. 使用正确的口令、证书或令牌登录普通用户，验证权限范围是否与设置一致。 4. 对用户进行口令、邮箱等基本信息进行修改，对用户权限范围进行修改。 5. 使用新的口令、证书或令牌登录普通账户，验证口令、基本信息、权限范围修改是否成功。 6. 退出所有登录账户。
预期结果： 1. 成功新建一个普通用户。 2. 口令、证书、令牌错误的情况下，用户无法登录系统。 3. 输入正确的口令、证书、或令牌成功后成功登录，所具有的权限范围和设定一致。 4. 用户可成功更改基本信息。 5. 重新登录时旧口令失效，新口令有效。修改用户基本信息成功。 6. 成功退出所有账户。
测试结果：
备注：

7.5.2 节点管理能力

用例编号：S201
用例分类：平台管理能力
验证目的：能够对合作节点进行调整。
预置条件： 1. 系统部署完成。 2. 登录管理员账户。
验证步骤： 1. 对合作节点进行增加，查看，上线，下线，删除。
预期结果： 1. 通过日志、抓包数据分析等方式，确定节点新增有通过签名等方式进行身份认证。 2. 增加的合作节点能够正常显示，并进行查看和后续的项目创建。 3. 能正常查看所有已经添加的节点。 4. 合作节点支持上下线操作，处于下线状态节点不能进行项目创建等操作。 5. 能正常删除合作节点，删除节点不可见，不能与其进行任何合作。
测试结果：
备注：

7.5.3 接口安全防护能力

用例编号：S301
用例分类：平台管理能力
验证目的：具备对外公开接口的安全限制和安全控制。
预置条件： 1. 系统部署完成。
验证步骤： 1. 提供接口开发规范和协议的相关说明文档，详细说明参数和调用方案，并模拟相关接口的访问及调用。 2. 模拟业务量突增变化、接口异常调用等操作。 3. 检查配置参数、抓包分析网络流量等操作。
预期结果： 1. 具备完整的接口开发规范和协议说明文档。 2. 模拟接口调用，接口的身份鉴别、访问控制、授权策略、审计等安全措施生效。 3. 检查配置参数、抓包分析网络流量等操作，说明跨安全域的接口调用采用了安全通道、加密传输等安全措施。
测试结果：
备注：

7.5.4 数据管理能力

用例编号：S401
用例分类：平台管理能力
验证目的：能够支持数据的导入和删除，以及相关权限的控制。
预置条件： 1. 系统部署完成。 2. 登录某个账户。
验证步骤： 1. 对数据进行增加，查看，删除。 2. 对数据进行权限的授予与删除。
预期结果： 1. 从外部数据（包括文件、mysql、hive 等常见数据源）增加新的数据进入系统，并能正常查看使用。 2. 赋予某项目的该数据的权限，项目能够正常使用该数据参与计算。 3. 删除该项目中对应数据的的权限，项目失去该数据的使用权利。 4. 能正常删除合作节点，删除后不能与被删除节点进行任何合作。
测试结果：
备注：

7.5.5 数据库支持能力

用例编号：S501
用例分类：平台管理能力
验证目的：验证能够支持主流数据库。
预置条件： 1. 系统部署完成。 2. 登录某个账户。
验证步骤： 1. 执行安全计算任务。 2. 更换数据库来源，重新执行安全计算任务。 3. 应支持常见数据库，包括但不限于 mysql、hive 等。
预期结果： 1. 更换数据库后，任务依然能够正常执行。 2. 系统可以正常支持常见数据库。
测试结果：
备注：

7.5.6 任务管理能力

用例编号：S601
用例分类：平台管理能力
验证目的：能够进行任务创建、任务调度和任务状态监控。
预置条件： 1. 系统部署完成。 2. 登录某个账户。
验证步骤： 1. 根据要求新建任务。 2. 查看任务状态。 3. 终止任务。 4. 查看任务日志。 5. 同时执行两个或两个以上任务。 6. 查看任务状态和任务日志。
预期结果： 1. 能够正常创建任务，任务正常执行。 2. 能够实时查看任务状态。 3. 能够实时终止任务。 4. 能够全面查看检索相关任务日志。 5. 能够支持两个或两个以上任务并行正常执行。

测试结果：
备注：

7.5.7 系统日志审计能力

用例编号：S701
用例分类：平台管理能力
验证目的：日志功能验证。
预置条件： 1、系统部署完成。
验证步骤： 1. 分别尝试登录系统。 2. 登录后进行基本操作，包括账户信息修改，增加删除数据，增加项目/任务。 3. 正常启动/运行安全计算任务，并顺利完成或中途终止任务。 4. 启动错误的安全计算任务。
预期结果： 1. 日志记录包含正常的登录，增删数据，增加项目/任务，启动任务。并能够快速检索相关的操作。 2. 日志记录包含用户异常登录等信息，并能够快速检索相关的操作。 3. 日志记录包含异常停止任务和错误的任务启动，并能够快速检索相关的状态和错误原因。
测试结果：
备注：

7.5.8 系统监控告警能力

用例编号：S801
用例分类：平台管理能力
验证目的：验证系统是否具有对异常状态具有监控告警功能。
预置条件： 1. 系统部署完成。 2. 登录某个账户。
验证步骤： 1. 配置数据监控指标告警项。 2. 正常启动和运行安全计算任务。 3. 观察告警效果。 4. 根据告警配置，提高相关输入从并超过告警阈值。 5. 观察告警效果。
预期结果： 1. 安全计算任务正常运行。 2. 相关监控指标符合期望。

3. 相关监控指标符合期望，能够反馈出异常情况。
测试结果：
备注：

7.5.9 网络容错能力

用例编号：S901
用例分类：平台管理能力
验证目的：验证系统在复杂网络环境的稳定性。
预置条件： 1. 系统部署完成。 2. 登录某个账户。
验证步骤： 1. 运行安全计算任务。 2. 主动短时间截断网络连接，模拟外网复杂环境。
预期结果： 1. 安全计算任务正常运行。 2. 能容忍短期的网络震荡，任务依然能够正常执行。
测试结果：
备注：

7.5.10 多数据方计算能力

用例编号：S1001
用例分类：平台管理能力
验证目的：验证系统提供超过两个数据方的隐私保护计算环境和能力。
预置条件： 1. 系统部署完成。 2. 登录某个账户。
验证步骤： 1. 执行某项安全计算任务（例如联合建模），至少有三个数据方（或以上）参与。
预期结果： 1. 任务正常执行，并能输出正确结果
测试结果：
备注：