隐私计算平台

亚信科技隐私计算平台 V1.5 白皮书

隐私计算帮助企业高效实现内外数据交互与价值挖掘，提升数据价值效能。

声明

任何情况下，与本软件产品及其衍生产品、以及与之相关的全部文件（包括本文件及其任何附件中的全部信息）相关的全部知识产权（包括但不限于著作权、商标和专利）以及技术秘密皆属于亚信科技（中国）有限公司(“亚信”)。

本文件中的信息是保密的，且仅供用户指定的接收人内部使用。未经亚信事先书面同意本文件的任何用户不得对本软件产品和本文件中的信息向任何第三方（包括但不限于用户指定接收人以外的管理人员、员工和关联公司）进行开发、升级、编译、反向编译、集成、销售、披露、出借、许可、转让、出售分发、传播或进行与本软件产品和本文件相关的任何其他处置，也不得使该等第三方以任何形式使用本软件产品和本文件中的信息。

未经亚信事先书面允许，不得为任何目的、以任何形式或任何方式对本文件进行复制、修改或分发。本文件的任何用户不得更改、移除或损害本文件所使用的任何商标。

本文件按“原样”提供，就本文件的正确性、准确性、可靠性或其他方面，亚信并不保证本文件的使用或使用后果。本文件中的全部信息皆可能在没有任何通知的情形下被进一步修改，亚信对本文件中可能出现的任何错误或不准确之处不承担任何责任。

在任何情况下，亚信均不对任何因使用本软件产品和本文件中的信息而引起的任何直接损失、间接损失、附带损失、特别损失或惩罚性损害赔偿（包括但不限于获得替代商品或服务、丧失使用权、数据或利润、业务中断），责任或侵权（包括过失或其他侵权）承担任何责任，即使亚信事先获知上述损失可能发生。

亚信产品可能加载第三方软件。详情请见第三方软件文件中的版权声明。

亚信科技控股有限公司（股票代码：01675.HK）

亚信科技是中国领先的软件产品及服务提供商，拥有丰富的软件产品开发和大型软件工程实施经验。公司深耕市场 30 年，在 5G、云计算、大数据、人工智能、物联网、数智运营、业务及网络支撑系统等领域具有先进的技术能力和众多成功案例，客户遍及通信、广电、能源、政务、交通、金融、邮政等行业。

2022 年，亚信科技完成收购商业决策服务领域的领先企业艾瑞市场咨询股份有限公司（「艾瑞咨询」），并整合形成新的"艾瑞数智"品牌。通过此次收购，亚信科技的核心能力从产品研发、交付服务、数据运营、系统集成延伸至咨询规划、智能决策，成为领先的数智化全栈能力提供商。

亚信科技始终致力于将 5G、AI、大数据等数智技术赋能至百行千业，与客戶共创数智价值。公司以"产品与服务双领先"为目标，产品研发围绕数智、云网、IT 及中台产品体系持续聚焦，实现行业引领，其中云网产品保持国际引领，数智产品实现国内领先，部分国际先进，IT 领域产品处于国内第一阵营。

面向未来，亚信科技将努力成为最可信赖的数智价值创造者，并依托数智化全栈能力，创新客户价值，助推数字中国。

部分企业资质

能力成熟度模型集成 CMM|5 级认证

信息系统建设和服务能力评估(CS4 级)

云管理服务能力评估证书卓越级

数字化可信服务 - 研运数字化治理能力认证

1S09001 质量管理体系认证证书

150200001T 服务管理体系认证证书

1S027001 信息安全管理体系认证证书

企业信用等级(AAA 级）证书

信息系统安全集成服务资质（二级）

信息系统安全开发服务资质（二级）

部分企业荣誉

连续多年入选中国软件业务收入百强榜单

连续多年入选中国软件和信息服务竞争力百强企业

中国软件行业最具影响力企业

中国软件和信息服务业最有价值品牌

中国软件和信息服务业最具影响力的行业品牌

中国数字与软件服务最具创新精神企业奖

中国电子信息行业社会贡献 50 强

中国人工智能领航企业

新型智慧城市领军企业

IDC 未来运营领军者

目录

1 摘要

数字经济时代，数据要素作为关键生产要素，聚合多维海量数据，充分挖掘并利用其内在价值，成为各产业发展的战略重点。随着《数据安全法》与《个人信息保护法》的相继发布，为各行业加强数据的合法使用与合规经营提供了指引，促进了整个数据产业的健康发展。2021 年以来，作为数据合法、合规使用保障的隐私计算技术在金融、政务、医疗、交通、能源等商业场景中迅速推广开来，为各行业发展数字经济带来新的契机、注入新的动能。

亚信科技推出了基于自主研发、技术领先的隐私计算平台，目的是让数据在技术信任机制下，以“可用不可见”的安全方式释放融合价值。平台采用业界首创的“1+X”隐私计算平台架构，提供了联邦学习建模、数据安全求交、匿踪安全查询和多方安全计算等功能。

另外，亚信科技与中国移动深入政府、金融、医疗等行业领域，利用联邦学习、多方安全计算等隐私计算技术，在“数据不出库、数据不落库”情况下实现跨行业数据融合，确保数据要素安全流动，避免用户隐私数据泄露，促进各行业实现数智化转型。

本白皮书将从产品概述、产品整体架构、产品功能架构、产品优势特性、产品价值、产品差异化优势、应用场景、产品客户成功故事、资质与荣誉等方面介绍。

2 缩略语与术语解释

隐私计算平台常见术语如表 2-1 所示。

表 2-1术语解释

缩略语或术语	英文全称	解释
FL	Federated Learning	联邦学习是一种分布式机器学习技术，通过在多个拥有本地数据的数据源之间进行分布式模型训练，在不需要交换本地个体或样本数据的前提下，仅通过交换模型参数或中间结果的方式，构建基于虚拟融合数据下的全局模型，从而实现数据隐私保护和数据共享计算的平衡，即“数据可用不可见”、“数据不动模型动”的应用新范式。
MPC	SecureMulti-Party Computation	多方安全计算指参与者在不泄露各自隐私数据情况下，利用隐私数据参与保密计算，共同完成某项计算任务。
PIR	Private InformationRetrieval	匿踪查询是安全多方计算中非常实用的一门技术与应用，可以用来保护用户的查询隐私，进而也可以保护用户的查询结果。其目标是保证用户向数据源方提交查询请求时，在查询信息不被感知与泄露的前提下完成查询。
PSI	Private Set Intersection	安全求交，全称隐私保护集合交集是指持有数据的两方能够计算得到双方数据集合的交集部分，而不暴露交集以外的任何数据集合信息。
SQL	Structured Query Language	结构化查询语言。SQL 是一种计算机语言,用来存储、检索和修改关系型数据库中存储的数据。
区块链	Blockchain	一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、防篡改、防抵赖的技术体系。

缩略语或术语	英文全称	解释
互联互通网络	interconnection network	不同隐私计算技术平台部署后相互连接，通过交互与协同形成的提供跨平台联合隐私计算服务的网络。
隐私计算	privacy-preserving computation	在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一系列信息技术，保障数据在流通与融合过程中的“可用不可见”。

3 产品概述

亚信隐私计算平台 AISWare MPC 基于数据资产管理、多方安全计算、联邦学习等数字化技术，实现数据可用而不可见，能够连接企业及行业数据孤岛，帮助企业构建可信数据流通与交易服务，避免用户隐私数据泄露，保障数据要素安全流通。

3.1 趋势与挑战

大数据是一把双刃剑。进入大数据时代，个人、企业和国家面临着隐私数据侵犯、数据泄露、数据勒索、数怕有滥用等一系列严重问题，数据安全与隐私保护紧密交织。

- 重要数据面临国家级对手威胁加大

国家级对手主动发起网络监视和侦察。我国关键信息基础设或将面临着被发起网络攻击的风险，造成重要数据被监听和窃取。

- 高价值特征敏感数据泄露风险加剧

黑客攻击政务数据可获取更高的利益回报。案例：2015 年，30 省社保系统遭遇黑客攻击，数千万信息泄露，可通过数据贩卖获取高额利润，并随意修改社保待遇、停发社保金。

- 互联网平台企业滥用信息

互联网平台企业滥采用个人信息，引发数据安全风险。移动应用强制授权、过度索权等问题严重，用户个人信息自主权丧失；基于数据有垄断优势进行“二选一”、“大数据杀熟”等，侵犯消费者权益。

- 数据贩卖严重侵害隐私

外部数据攻击利用爬虫等技术窃取并倒卖个人数据。如 XX 视频网站遭受黑客攻击，数千万条用户数据泄露并在“暗网”以高价出售。“内鬼”常成为非常数据交

易链源头。如，XX 快递内鬼倒卖四十万条公民生名、地址、手机号和所购物品等信息。

但是，数据价值一定要流转。数据要素流转目前主要面临三个问题：不敢共享、不会共享、不愿共享。一是由于数据安全和法律责任不清而“不敢共享”；二是由于技术标准和应用场景不明而“不会共享”；三是由数据要素的确权定价与利益分配问题导致“不愿共享”。

3.2 产品定义

隐私计算，是指在保证数据提代方不泄露原始数据的前提下，对数据进行分析计算，有效提取数据要素价值的一类信息技术，保障了数据在产生、存储、计算、应用、销毁等各个环节中的“可见不可见”。

参与方在不泄露各自数据的前提下，通过协作对他们的数据进行联合机器学习和联合分析。隐私计算的参与方既可以是同一机构的不同部门，也可以是不同的机构。在隐私计算框架下，参与方的数据明文不出本地，在保护数据安全的同时实现多源数据跨域合作，以破解数据保护与融合应用难题。涉及密码学、分布式计算、人工智能、数据科学等众多领域。

3.3 产品定位

隐私计算技术通过不交互原始数据、只流通数据价值的方式，在一定程度上回避了数据权属争议、降低了数据流转过程中的安全风险，为数据要素流通提供了新模式。

- 助力数据价值释放

企业搭建隐私计算平台，一是对内能将隐私计算能力办理出到企业上下，提从给集团及成员单位应用，融合各级公司、各部门的数据能力，充分发挥内部数据价值;二是对外能够通过数据交换建立完备的数据生态,即通过隐私计算技术，消除各方对于数据安全及合规使用的担忧，从而与外部数据源展开充分合作，引入各类具有价值的外部数据，建设可持续发展的数据生态。

- 算法赋能数据价值

各方约定算法规则，数据在这组规则下运行，最后得到可用于数据业务的模型。因此，算法实际上规定了数据使用目的和方式。当前算法正逐渐演变为核心商业秘密，因此在数据生态建设过程中，可将算法参数作为隐私数据处理，以“可用不可见”方式对外提供使用。

- 提供密文算力服务

计算方为数据生态提供算力支持，其角色如同数据生态的基础设施承建方。实践中，一个计算方会部署一个计算集群，通过增加集群内机器节点数量提高其算力水平。在某些密文计算协议中，需多个计算方相互监督才能实现计算协议安全，如基于秘密分享的协议。

4 产品整体架构

隐私计算平台基于数据资产管理、多方安全计算、联邦学习、区块链等数字化技术，实现数据可用而不可见，能够连接企业及行业数据孤岛，帮助企业构建可信数据流通与交易服务，避免用户隐私数据泄露，保障数据要素安全流通。

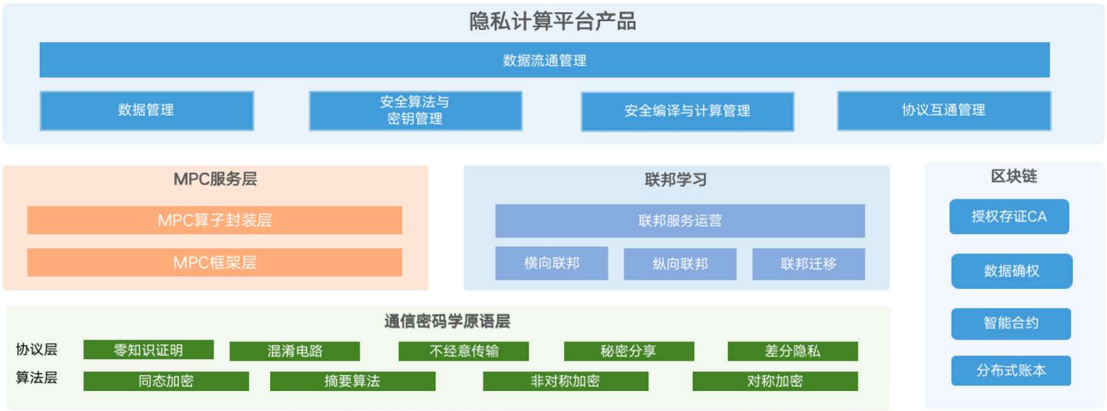


图 4-1 产品整体架图

- 通信密码学原语层：利用密码学技术和分布式共识协议保证网络传输与访问安全，实现数据多方维护、交叉验证、全网一致、不易篡改。
- MPC 服务层：利用 MPC 框架层，对 MPC 算子，如隐匿查询、安全求交、多方安全云计算进行封层应用。
- 联邦学习：通过联邦学习框架层，可进行横向联邦、纵向联邦等算法应用。
- 区块链：将区块链与隐私计算结合，可保证整个过程是可审计、可验真的。能够完成可信身份认证、数据确权、数据计算过程追踪、基于权属和计算过程的数据价值自动分配等。
- 数据流通：是将各个参与方的数据进行数据同步、数据授权、数据计算等流程管理。

5 产品功能架构

亚信隐私计算平台的产品架构，主要是基于平台的容器化、虚拟机等部署的基础上，实现平台管控的互联互通协议管理功能，与业务构建的功能。再利用算法层的多方计算、安全求交、匿踪查询、可信执行环境，完成隐私服务层，平台运营层。

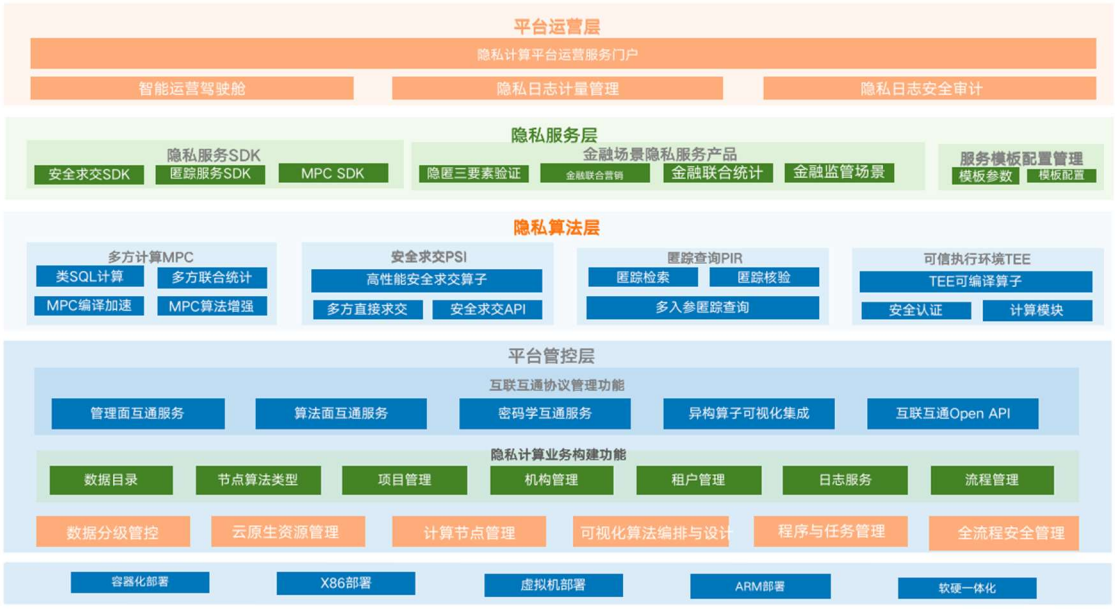


图 5-1产品功能架构图

- 平台运营层：是针对平台的相关业务数据进行统计分析，包括运营服务门户、智能运营驾驶舱、隐私日志计量管理、隐私日志安全审计。
- 隐私服务层：服务层包含三方面，一是隐私服务 SDK、二是服务产品，三是服务模板配置管理。
- 隐私算法层：对隐私计算的算子，如多方计算、安全求交、匿踪查询等进行算子算法优化，并且通过可信执行环境，保证隐私安全。
- 平台管控层：主要是对平台的业务功能、算法协议、以及涉及算法的界面操作的管理。

5.1 基础功能

隐私计算的基础功能主要针对是业务构建功能，如项目管理、租户管理、流程管理等。

- 项目管理：对参与方的项目进行统一管理，本方项目支持通过新增、编辑的操作；合作方项目进行同步的操作。
- 租户管理：支持多租户模式，租户间数据与计算完全隔离，保证每个客户的数据与计算安全稳定。
- 流程管理：对平台的数据授权、项目授权、程序运行申请等统一管理，支持通过 API 方式进行多方的授权审批。
- 运营服务门户：隐私计算运营服务门户主要是根据数据集的信息，进行合作入驻的申请，同时支持对入驻进度的查询等功能。
- 管理面互通服务：实现参与方的身份管理、数据资产的管理和确权，整个使用流程的可追溯等，实现数据用途可控可计量。
- 互联互通 Open API：对于通信协议、资源管理、任务调度、算法协同等互联互通的基础环节形成统一共识，提出标准化的技术规范，对外开放 API。
- 数据分级管控：数据分类分级、安全策略等数据安全管理体系建设，实现数据的安全治理和全生命周期的防护。

- 智能运营驾驶舱：智能运营驾驶舱主要是对合作运营的整体情况、双方机构的运营情况进行分析。支持对各方合作运营的数据、项目、算子算法、任务监控等内容的统计。

- 日志服务：对日志全程审计的日志管理，对 API、硬件资源、平台使用的监控管理；平台应具备对数据和模型的访问、使用、授权等系统日志的记录与审计能力。

5.2 特色功能

隐私计算平台的特色功能包括了安全求交 SDK、高性能安全求交算子、多方直接求交、安全求交 API 的功能。

5.2.2 安全求交 SDK

通过安全求交的服务创建，并生成 SDK，由客户端安装 SDK，从而来完成双方的求交任务。

- 服务创建：对安全求交服务创建，包括安全求交服务的基本信息、数据集获取等功能；新增后，支持对服务的发布、授权等功能。

- 服务运行：对服务授权后，将安全求交服务下载安装，可对 SDK 服务进行求交能力的运行，并产生日志。

5.2.3 高性能安全求交算子

通过优化的计算资源，如内存的优化，以实现安全求交算子的高性能处理能力，实现亿级的数据计算。

- 支持程序编排，获取安全求交所需组件；支持组件的配置功能，取双方的有交集的数据集进行配置；支持组件的配置功能，取双方的无交集的数据集进行配置。
- 支持安全求交程序运行，获取安全求交程序的运行结果。
- 查看计算资源的使用情况。

5.2.4 多方直接求交

多方安全求交针对三方隐私交集、两方隐私差集和三方隐私并集等运算，以得到最终的安全求交的结果。

- 两方隐匿查询：将两方的数据集进行隐匿查询，并得到查询结果，具有保护被查客户的信息。
- 两方隐私差集：通过将两方的数据集，得到数据求交以外的本方数据信息，也就不在合作方里的数据集。
- 三方隐私交集：支持通过三方数据集，进行两两求交，并最终得到求交的结果。
- 三方隐私并集：支持通过三方的数据进行安全求交，并最后得到三方求交的并集结果。

5.2.5 安全求交 API

通过将安全求交能力封装成 API，并且在 API 的发布和授权的情况下，由客户进行调用。

- 支持安全求交服务定义；安全求交服务授权，授权后可进行安全求交；安全求交服务未授权，未授权则不能安全求交。
- 支持安全求交 API 获取求交参数;支持安全求交根据参数进行能力运行，获取安全求交的运行结果。
- 支持 API 调用日志的查看。

6 产品优势特性

隐私计算平台特性主要包括了自研安全求交技术提升性能、跨平台的互联互通、自研基于密码学协议的隐私信息查询等。

6.1 自研安全求技术能力达到国内领先

安全求交属于隐私计算领域的特定应用，它的实现是基于隐私保护集合求交(Private Set Intersection-PSI)技术，允许持有各自集合的两方或多方来共同计算各自集合的交集运算；在协议交互的最后，一方或是多方根据预先约定得到正确的交集，而且不会得到交集以外其他方集合中的任何信息。

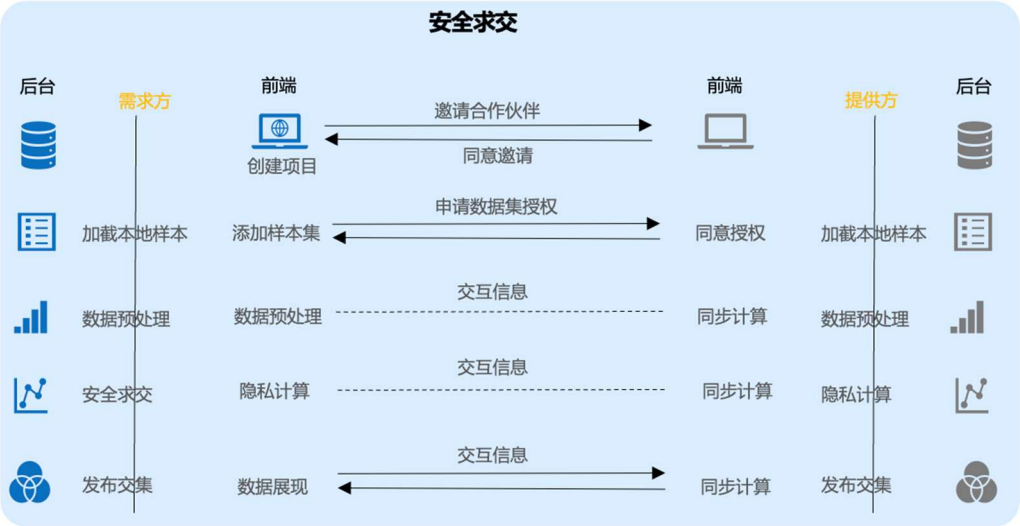


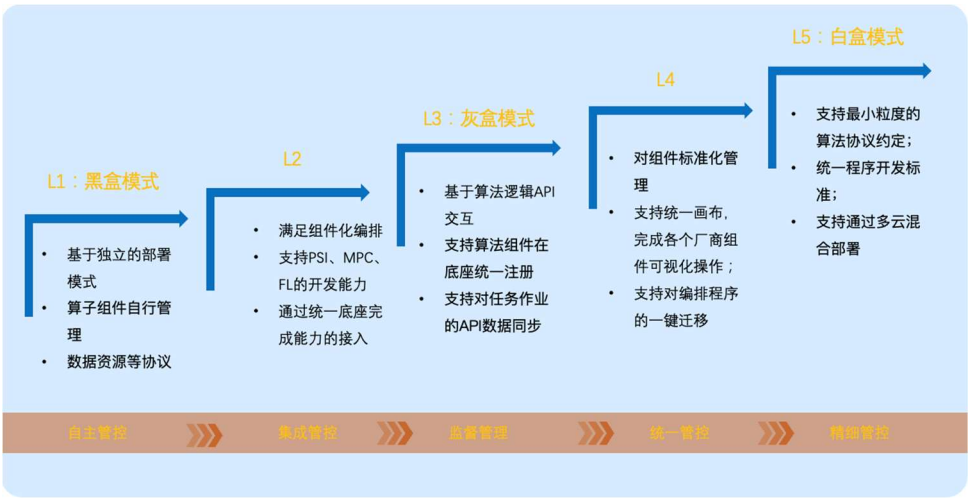
图 6-1 安全求交的算法应用

- 构建基于不经意传输扩展的伪随机函数用来完成数据比对，并使用布谷鸟 hash 算法减少传输数据量。
- 与基础的不经意传输算法实现的 PSI 相比，性能大幅提升，网络开销大幅下降。
- 开源最广泛使用的 FATE 技术能力，计算性能可以提升 50%以上。

6.2 隐私计算跨平台互联互通能力增强

隐私计算平台从业务价值出发，推动互联互通的标准化进程，技术上实现互联互通时，始终要突出安全，坚守安全底线，分别从自主管控、集成管控、监督管控、统一管控、精细管控的进行程进行演进，确保互联互通能够在安全的基础上向前推进，既可以满足互联互通功能，又满足数据安全流通。

图 6-2 互联互通演进



- 提供统一的接入、管理、监控和运维等方面的要求和指导，为隐私计算平台间的互联、互通提供一个可以参考的标准规范。
- 支持黑盒、白盒、灰盒多种互通模式，以递进式实现互联互通的安全可视化，提高了安全层面的可解释性，让用户掌握更强的系统运营能力。
- 从黑盒变成灰盒，灰盒变成白盒，多种互通模式的转变实现了多边信任增强，提升了各行业隐私计算互通效率。

6.3 基于密码学协议的隐私信息检索实现

匿踪查询作为隐私计算领域中安全多方计算下的子分支，可以用来保护用户的查询隐私，使数据持有方无法获知具体查询对象，从而很好地保护查询方的隐私信息，打消安全顾虑，促进数据安全有序流通。

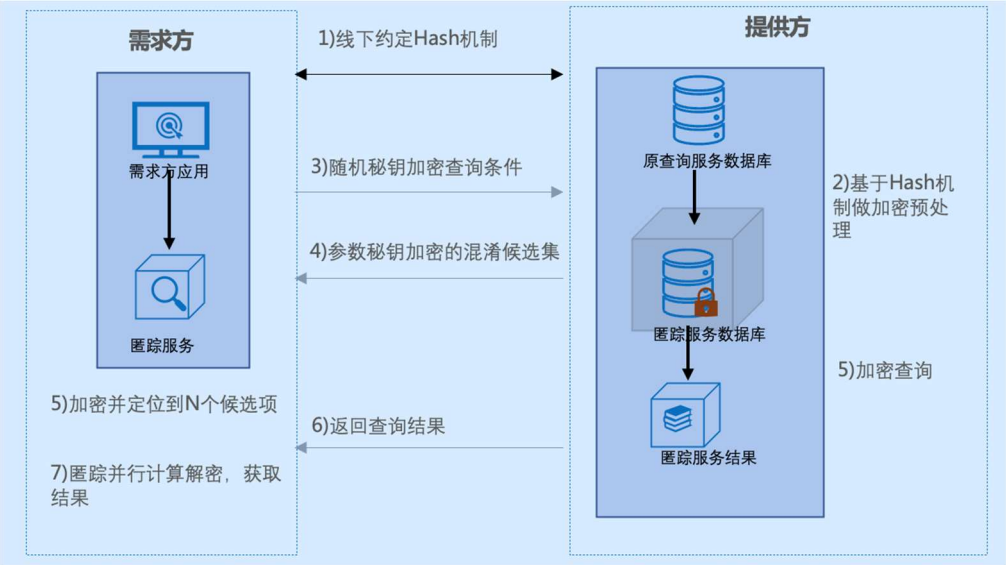


图 6-3 匿踪查询算法应用

- 利用 RSA 非对称加密、不经意传输等密码学技术，构建出多方查询时的数据交互加密通信通道。
- 在整个查询交互过程中进行数据混淆、数据加密、数据传输、数据解密及匹配，从而让数据服务方无从知晓查询方的查询信息。
- 查询方无从知晓数据服务方除查询信外的其余信息，达到数据隐私保护、防止信息泄露、制止数据缓存的目的。

6.4 隐私计算智能化驾驶舱，实时感知运营态势

运营驾驶舱主页以大屏的方式呈现，通过首页查看整体运营情况，再根据中心节点与合作节点，查看项目信息、以及任务运行情况。

图 6-4 智能运营驾驶舱

7 产品价值

隐私计算，是参与方在不泄露各自数据的前提下通过协作对他们的数据进行隐私求交、隐匿查询、多方计算、联邦学习。同时，隐私计算技术在政府端、企业端和个人端都发挥着巨大的作用，能够解决现阶段数据保护和数据流通多方面痛点。

- 盘活企业数据资产，发挥数据经济价值。

以隐私计算为代表的密态数据流通技术的蓬勃发展，使得密态数据流通成为重要的数据流通形式。帮助大量拥有数据的企业（运营商、大型企业），基于隐私计算技术打造隐私计算服务平台，进行合规可信的数据流通与交易，满足大型企业数据合规监管。

- 跨行业数据融合，赋能产业数字创新。

缔造跨行业跨平台可信数据流通标准，通过隐私计算互联互通标准化接口，实现数据合规融合分析，助力产业实现精细管理、精益生产、精准营销、精确规划，赋能产业数字化转型升级。

- 可信数据流通，推动数据要素市场化配置。

隐私计算，如多方安全计算及联邦建模，可以保障原始数据不脱离数据持有方的控制范围，可助力可信数据流通交易，促进产业数据要素价值释放，以隐私计算和可信数据流通运营为聚焦点，推动数据要素市场化配置。

8 产品差异化优势

隐私计算不同类型的技术路线各具能力优势，将满足差异化的客户选型需求。不同的场景需求下，应该为客户提供差异化的技术方案或技术组合方案，进而实现安全性与性能的有效平衡。

- 业界首创隐私数据计算“1+X“架构，支持异构算法一键集成。

亚信隐私计算平台采用 1+X 架构（1 个技术底座，X 个算法），通过统一技术底座集成亚信自研和其他各厂商的隐私计算组件、区块链和数据中台，有助于运营方引入多样化的合作伙伴，打造一体化的数据开放生态。

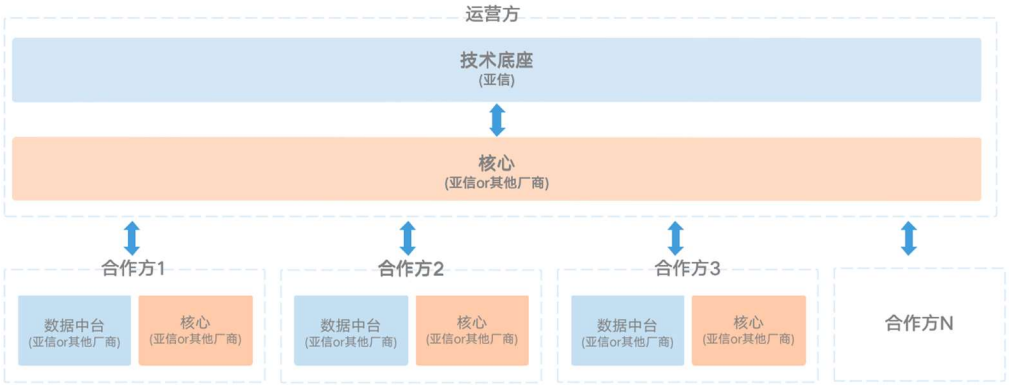


图 8-1 1+X 集成架构

- 体系化的共享机制，适配不同的数据安全流通场景。

隐私计算，是实现隐私数据共享的综合性业务处理平台。在保护数据提供方隐私信息的前提下，具备安全、正确的基于密码理论的可靠性；具备多技术路线、

丰富场景磨合的丰富性；具备高规格、高可用的安全计算性；具备适配全国产化、独立自主研发的创新、安全性。

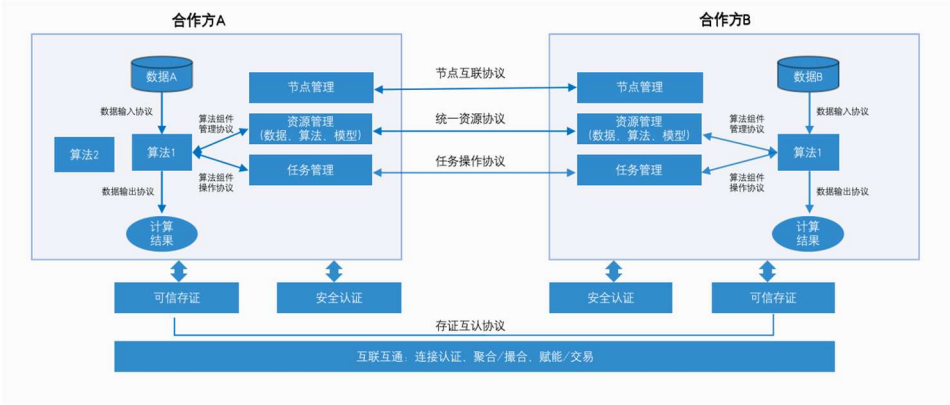


图 8-2 数据流通

- 运营一体化平台，为各个领域提供数智化服务，构建服务生态。

搭建了统一规范、互联互通、安全可控的数据开放环境，多方协同全程加密传输、缓存和运算，保护数据的安全和隐私，促使数据流通价值最大化，安全合规的推动跨部门、跨机构、跨行业的数据开放与共享。

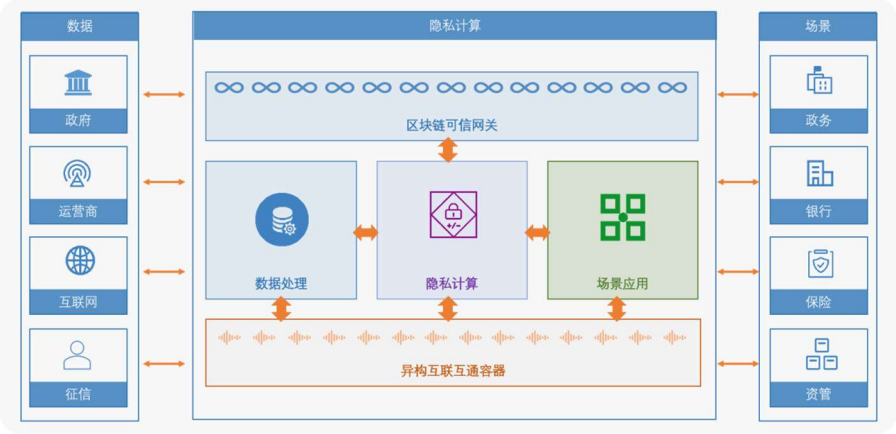


图 8-3 数智化服务

9 应用场景

在运营商、银行、保险、政务、教育、电商等众多行业的业务场景中，都会涉及到跨机构、跨部门的数据合作，但数据隐私泄露问题又是一个长期无法逾越的障碍。亚信科技隐私计算平台正好完美地解决了这个问题，只需在合作方之间传递加密中间参数即可完成联合建模，最大化保障了合作方之间的数据安全。

9.1 场景综述

隐私计算平台技术在原始数据不出库的条件下，实现数据"价值"和"知识"流通的目标，以此促进跨领域多维度数据的融合，构建"数据可用不可见"的合作新模式。目前业内主要基于匿踪查询、安全求交、联合统计、联邦学习等技术进行商用场景落地。

9.2 匿踪查询

通过隐私计算，查询方可隐藏被查询对象关键词或客户 ID 信息，数据提供方提供匹配的查询结果却无法获知具体对应哪个查询对象。数据不出门且能计算，杜绝数据缓存、数据泄露、数据贩卖的可能性。

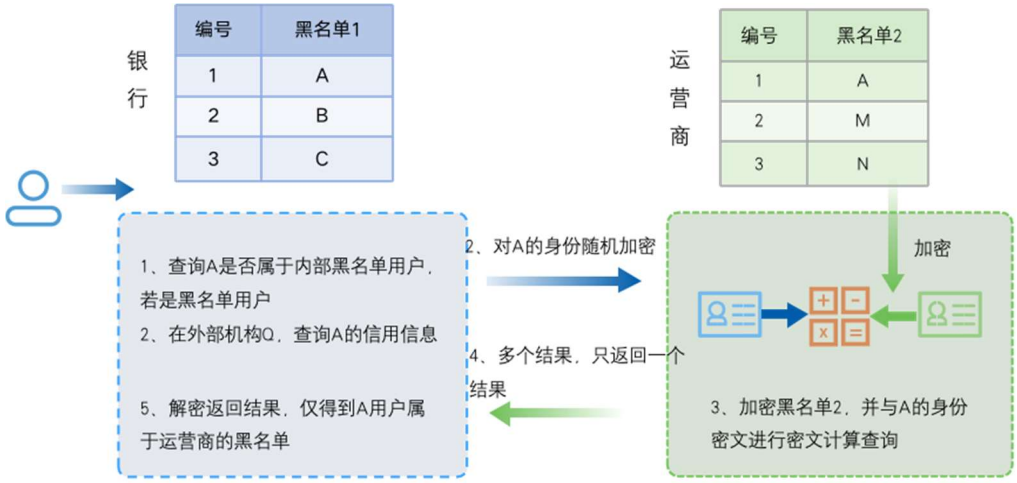


图 9-1 场景-匿踪查询

9.3 安全求交

通过隐私计算，持有各自集合的两方来共同计算两个集合的交集。在协议交互的最后，一方或是两方应该得到正确的交集，而且不会得到交集以外另一方集合中的任何信息。

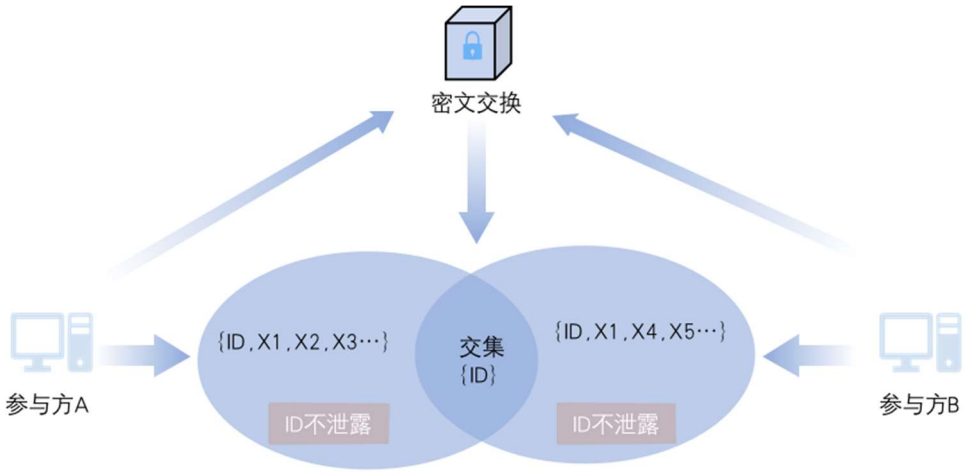


图 9-2 场景-安全求交

9.4 联合统计

通过隐私计算，可使多个非互信主体在数据相互保密的前提下进行高效数据融合计算，达到"数据可用不可见"，最终实现数据的所有权和数据使用权相互分离。

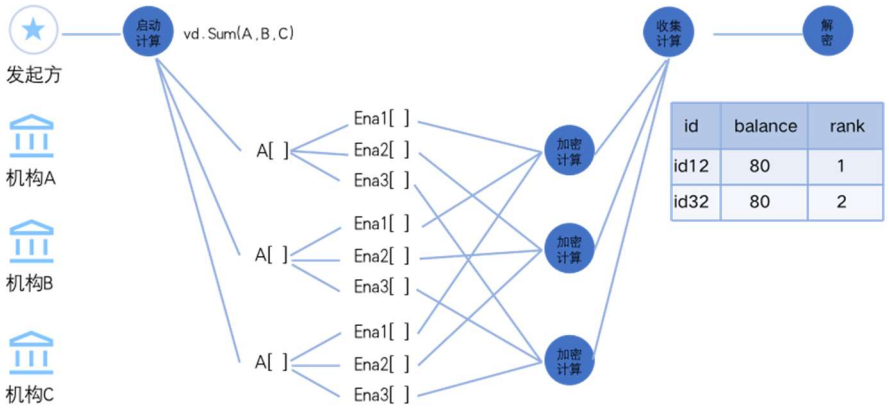


图 9-3 场景-联合统计

当用户向银行提出贷款申请时，银行需要评估借贷风险，排查当前用户是否有多头借贷、和超额借贷的风险。考虑隐私安全的问题，银行联合多家同行、跨

行，通过隐私计算平台，在贷前对用户各银行的借贷总额进行联合统计。银行收到联合统计结果后，决定是否向用户发放贷款。

9.5 联合建模

隐私计算保证参与方在整个计算过程中难以得到除计算结果之外的额外信息，也难以逆推原始输入数据和其他隐私信息。在完成模型训练的同时，满足隐私合规要求。

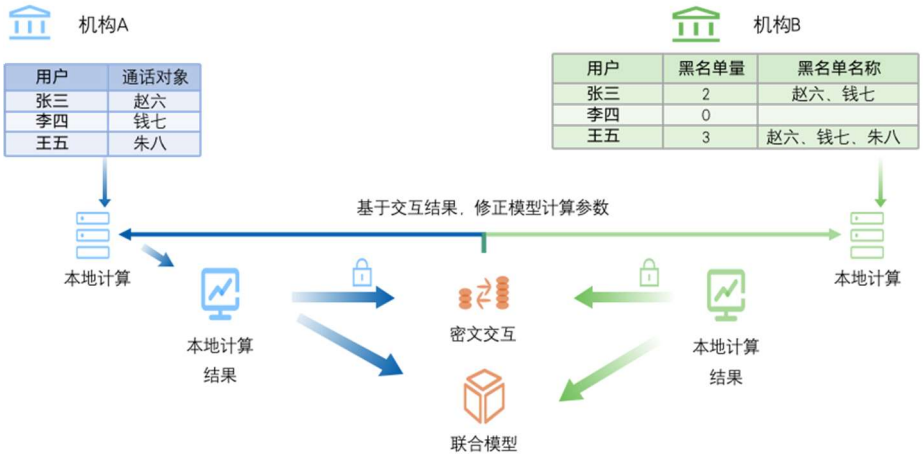


图 9-4 场景-联合建模

“以非法占有为目的，利用电话、短信、聊天工具等手段“的电信诈骗联合建模，涉及到运营商、银行、公安等多个领域。针对电信反欺诈识别的联邦模型，将运营商的用户等级、社交、业务变化情况，与公安的诈骗号码进行联合建模型，实现电信欺诈联合预测，输出电信诈骗名单。

10 产品客户成功故事（应用案例）

本章节将对成功案例进行具体介绍。

10.1 基于运营商标签的金融精准营销

电信行业的数据包括上网信息、语音/短信信息、消费记录、位置信息、终端信息、用户身份信息等，在数据确权的情况下，可与证券行业进行融合，对用户画像、风险等级、精准营销等方面进行分析。

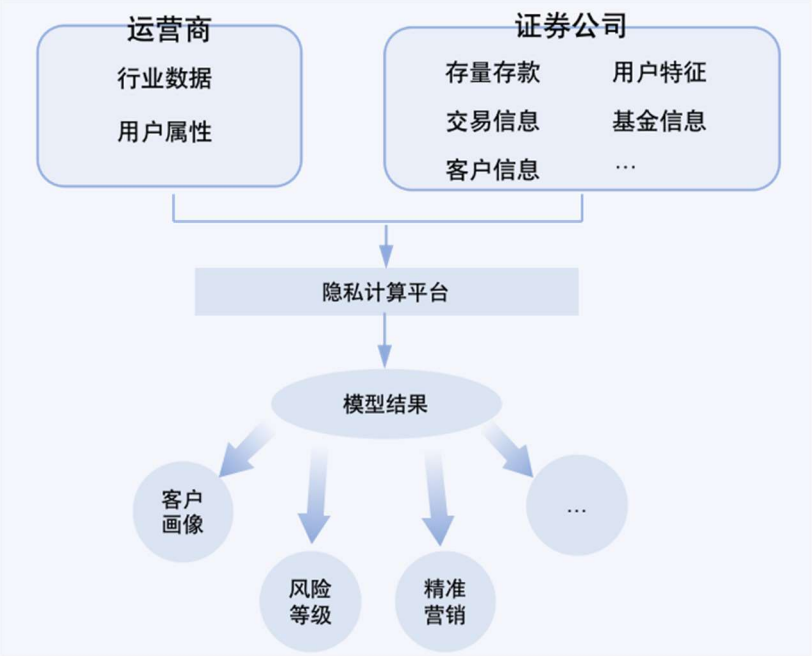


图 10-1 基于运营商标签的金融精准营销

- 业务痛点：政策合规要求和同行业竞争导致客户信息在本行业内流通困难，导致在客户体量和地域分布上的局限性。
- 解决方案：将外部多方数据接入隐私计算平台，从客户支付行为、常用设备、通信情况等判断数据的风险等级。

- 实施效果：与他行业的数据融合，可有效防止他行业的骚扰电话、垃圾短信；多方计算、联邦学习等技术的联合应用，可以对计算数据、过程、结果进行追踪审计，增强监管方穿透力和有效性。

10.2 金融行业的信贷场景应用

在银行信贷业务整个闭环中，从引流阶段的营销服务，到贷前、贷中、贷后全面风控服务，隐私计算平台衔接各方数据能力，在保障各方数据隐私安全的基础上助力银行信贷业务顺利展开。

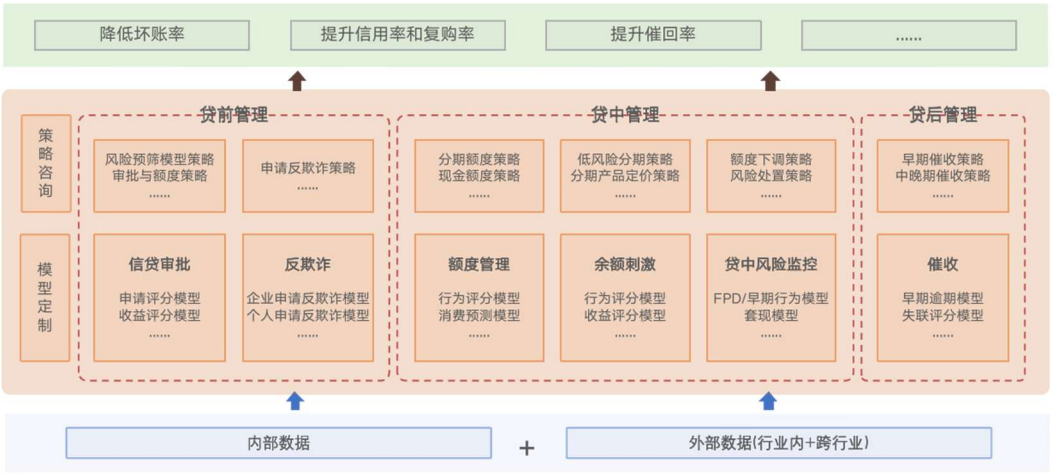


图 10-2 金融行业的信贷场景应用

- 业务痛点："数据孤岛"现象使金融机构在贷前、贷中、贷后各环节都存在风险识别难的痛点问题，且多头借贷风险较难规避。

- 解决方案：利用隐私计算技术，银行、证卷等金融机构间，可以实现数据安全融合，在贷款全周期流程中实时、精准、全面地分析客户。

- 实施效果：通过采用纵向联邦学习、多方安全计算等技术，将双方数据共同用于训练联邦风控模型，在保护用户隐私数据的前提下实现模型优化，

进而更好地支持普惠金融和消费金融发展，提高风控能力，且数据样本和模型效果的提升还可有效节约传统信贷的审核成本。

11 资质与荣誉

多方安全计算的基础能力已通过信通院的专项测评，包括计算相关基础能力测试、编译及计算功能测试、数据流通相关管理功能；同时包括产品安全性、健壮性、稳定性相关测试、性能等方面的测试，均满足多方安全计算基础能力测试要求。


CAICT 中国信通院　可信隐私计算评测　TTL泰尔实验室

证书编号：IY2022101380　　颁发日期：2022年7月13日

多方安全计算
基础能力专项评测证书

亚信科技（中国）有限公司

单位地址：北京市海淀区中关村软件园二期西北旺东路10号院东区亚信大厦
产品/服务名称：亚信隐私计算平台 AISWare MPC
产品版本号：V1.0
软著登记号：2022SR0548020
符合标准：BDC 26-2021《基于多方安全计算的数据流通产品 技术要求与测试方法》

经检验，贵单位的"亚信隐私计算平台 AISWare MPC V1.0"，于中国信通院开展的第1批可信隐私计算评测中，在计算相关基础能力测试、编译及计算功能测试、数据流通相关管理功能、产品安全性、健壮性、稳定性相关测试、性能等方面，均满足多方安全计算基础能力测试要求，详见测试报告（报告编号：V22Y10138），特发此证。

（本证书真实性依据评测机构定期监督获得保持，证书真实性信息请登录www.datobench.cn查询。）
【由于该评测是针对2022年7月1日前该大数据产品情况进行的披露，用户依然应留意在具体使用过程中可能发生的风险。因多方安全计算技术快速发展，产品/服务不断升级迭代，标准规范随行业发展不断更新等原因，当产品或评测标准发生较大变化时，建议亚信隐私计算平台 AISWare MPC产品重新评测，中国信息通信研究院将在2023年7月组织新一批评测。】

签发人：

签发日期：2022年7月1日

中国信息通信研究院
中国泰尔实验室
地址：北京市海淀区花园北路52号

图 11-1 多方安全计算基础能力专项评测证书

联邦学习的基础能力已通过信通院的专项测评，包括调度管理能力、数据处理能力、算法实现、效果及性能、安全性等。将适用范围和应用场景拓展到了人工智能领域，同时实现了性能、安全性与兼容性等方面的多重提升，具有多项领先的技术优势和独创的功能特点。

CAICT 中国信通院　可信隐私计算评测　TTL泰尔实验室

证书编号：IYB-2021-20282　　颁发日期：2021年12月20日

联邦学习
基础能力专项评测证书

亚信科技（中国）有限公司

单位地址：北京市海淀区西北旺东路10号院东区19号楼
产品/服务名称：亚信科技联邦学习平台AISWare AI² FL
产品版本号：V1.0
软著登记号：2020SR0281880
符合标准：BDC 41-2020《基于联邦学习的数据流通产品 技术要求与测试方法》

经检验，贵单位的"亚信科技联邦学习平台AISWare AI² FL V1.0"，于中国信通院开展的第5批可信隐私计算评测中，在调度管理能力、数据处理能力、算法实现、效果及性能、安全性等方面，均满足联邦学习基础能力测试要求，详见测试报告（报告编号：V21Y20282），特发此证。

（本证书真实性依据评测机构定期监督获得保持，证书真实性信息请登录www.databench.cn查询。）
【由于该评测是针对2021年12月20日前该大数据产品情况进行的披露，用户依然应留意在具体使用过程中可能发生的风险。因联邦学习技术快速发展，产品/服务不断升级迭代，标准规范随行业发展不断更新等原因，当产品或评测标准发生较大变化时，建议亚信科技联邦学习平台AISWare AI² FL产品重新评测，中国信息通信研究院将在2022年12月组织新一批评测。】

签发人：

签发日期：2021年12月13日

中国信息通信研究院
中国泰尔实验室
地址：北京市海淀区花园北路52号

图 11-2 联邦学习基础能力专项评测证书

12 联系我们

亚信科技（中国）有限公司

地址：北京市海淀区中关村软件园二期西北旺东路 10 号院东区亚信大厦

邮编：100193

传真：010-82166699

电话：010-82166688

Email：5G@asiainfo.com

网址：www.asiainfo.com

Thank you

亚信科技依托产品、服务、运营、集成能力助力企业数字化，持续创造新价值。