上海市浦东新区市场监督管理局
上海市浦东新区人民政府电子政务办公室

浦市监标计〔2023〕217号

关于发布浦东新区标准化指导性技术文件《公共数据授权运营可信环境技术规范》的通知

各有关单位:

上海市浦东新区标准化指导性技术文件《公共数据授权运营可信环境技术规范》已经区政府批准，现予以发布。

文件编号及名称为:

DB 31115/Z 040—2023 公共数据授权运营可信环境技术规范

以上文件自2023年12月15日起实施。

特此通知。

上海市浦东新区
市场监督管理局

上海市浦东新区人民政府
电子政务办公室
2023年12月15日

ICS 35.020
CCS L 77

上海市浦东新区标准化指导性技术文件

DB 31115/Z 040—2023

公共数据授权运营可信环境技术规范

Technical specification for trusted environment of authorized operation of public data

2023-12-15 发布　　2023-12-15 实施

上海市浦东新区人民政府电子政务办公室
上海市浦东新区市场监督管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1-2020给出的规定起草。

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。

本文件由上海市浦东新区人民政府电子政务办公室提出并组织实施。

本文件由上海市浦东新区人民政府电子政务办公室归口。

本文件的起草单位：上海市浦东新区大数据中心、上海数字产业发展有限公司、云赛智联股份有限公司、上海富数科技有限公司、华为技术有限公司、蚂蚁区块链科技（上海）有限公司、杭州锘崴信息科技有限公司、上海财经大学、上海梦创双杨数据科技股份有限公司、上海达网科技有限公司、上海仪电鑫森科技发展有限公司、北京航空航天大学杭州创新研究院、上海零数众合信息科技有限公司、南湖实验室、普元信息技术股份有限公司、星环信息科技（上海）股份有限公司。

本文件主要起草人：宋卫华、徐瑾伦、黄得志、史锋、尹洪刚、聂影、陈豪、张宁、陈正伟、章建兵、周海涛、史进、卞阳、李倩、方竞、叶飞、杨小强、余正华、昌文婷、周斌、李帜、王帅、韩景倜、杨剑、宋汝良、彭向亮、高文娟、易泽坤、刘辉、江晓峰、郭振纬、罗正球、兰春嘉、杨珍、陆一凡、张磊、夏佳斌、肖梅、许兴欣、唐恺。

本文件于2023年12月首次发布。

引　言

公共数据运营是盘活公共数据资源、挖掘数据价值、释放数据红利的重要手段。《上海市数据条例》提出本市建立公共数据授权运营机制，提高公共数据社会化开发利用水平。被授权运营主体应当在授权范围内，依托统一规划的公共数据授权运营平台提供的安全可信环境，实施数据开发利用，并提供数据产品和服务。浦东新区作为社会主义现代化建设引领区，率先建立公共数据授权运营安全可信环境，推动公共数据社会化开发利用，本文件结合浦东新区公共数据运营探索实践，提出公共数据授权运营可信环境的相关技术规范。

公共数据授权运营可信环境技术规范

1 范围

本文件确立了公共数据授权运营可信环境的通用要求、业务流程、总体架构、技术要求、应用场景等相关要求。

本文件适用于指导浦东新区公共数据授权运营可信环境的技术要求。

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 37721-2019 信息技术 大数据 分析系统功能要求

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

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

公共数据 public data

本市国家机关、事业单位、经依法授权具有管理公共事务职能的组织、以及供水、供电、供气、公共交通等提供公共服务的组织，在履行公共管理和服务职责过程中收集和产生的数据。

3.2

公共数据授权运营 authorized operation of public data

指依法授权符合规定条件的主体使用、加工各级行政机关以及履行公共管理和服务职能的事业单位在依法履行职责过程中采集和产生的各类数据资源的活动。

3.3

公共数据授权运营可信环境 trusted environment of authorized operation of public data

针对公共数据授权运营活动，在政务外网建设的软硬件安全区域，运用区块链、隐私计算等技术，保证数据开发、流通、运营和监管等环节的数据安全性。

3.4

公共数据授权运营平台 platform for authorized operation of public data

指依托安全可信环境，实施公共数据开发利用，并提供数据产品和服务的技术平台。

3.5

公共数据授权运营域 domain for authorized operation of public data

指依托公共数据授权运营平台，承载多租户数据托管、多源数据融合处理、模型训练推理、内部数据受控访问等服务的特定安全域，提供算力算法、可信流通等服务，具备安全脱敏、访问控制、监

管溯源、封存销毁、全程审计等合规监管功能。

3.6

数据产品 data product

指通过对原始数据资源或融合数据资源进行加工处理、分析研究所形成的，能够发挥数据价值的产品。数据产品在安全合规前提下，能够参与社会生产经营活动并为使用者或所有者带来经济效益。

3.7

数据服务 data service

指基于数据需求，利用软硬件产品及技术，通过数据相关平台建设、数据融合、治理、交付、评估等，将原始数据加工成数据产品，并提供给数据产品需求方的服务过程。

3.8

可信执行环境 trusted execution environment

指通过软硬件方法在中央处理器中构建一个安全区域，采用可信计算和虚拟化等隔离技术，为安全敏感数据/应用提供一个可信赖的执行环境，同时保护安全区域加载的程序和数据的机密性和完整性的一种技术手段。

3.9

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漏各方隐私数据的密码技术。

[来源：JR/T 0196-2020，3.1]

3.10

联邦学习 federated learning

一种多个参与方在保证各自原始数据不出数据方定义的可信域的前提下，获取各方所需的计算结果，协作完成某项机器学习任务的模式。

3.11

管理方 management unit

管理公共数据授权运营的政府组织机构。

3.12

数据提供方 supply unit for public data

生产、提供公共数据的组织机构。

3.13

数据需求方 demand unit for public data

申请、使用公共数据的组织机构。

3.14

授权运营方 authorized operation unit for public data

对公共数据的日常运营情况进行管理，对接数据需求方的需求，并将数据服务结果提供给数据需求方的企业或机构。

3.15

技术提供方 technical service unit

在公共数据授权运营平台上，提供各类软件、硬件、算法以及算力产品的企业或机构。

3.16

服务开发方 develop service unit

根据数据运营方提出的需求，利用技术服务方提供的产品，将公共数据加工成数据产品的企业或机构。

4 缩略语

下列缩略语适用于本文件。

CPU 中央处理器（Central Processing Unit，CPU）

MPC 多方安全计算（Secure Multi-Party Computation）

P2P 对等网络（Peer to Peer）

5 公共数据授权运营可信环境通用要求

5.1 可靠性

公共数据授权运营可信环境应符合以下可靠性要求：

a) 系统及组件（如操作系统、网络、数据库、软件）应具备数据的备份恢复能力，在出现故障时可根据备份数据完成系统的故障修复；

b) 系统在数据备份期应可持续提供服务；

c) 应具备主动风险识别机制。

5.2 兼容性

公共数据授权运营可信环境应符合以下兼容性要求：

a) 应支持主流技术与标准；

b) 应支持系统的兼容性升级，并能正常提供服务；

c) 应支持相关硬件集成能力，通过集成相关硬件设备提升系统能力，如区块链一体机、可信芯片、加速卡、专用集成电路等；

d) 配备的计算和存储资源量应满足系统常规和高峰时期运行需求，存储设备应支持主流存储协议；

e) 系统应支持在主流操作系统上稳定、流畅运行。

5.3 扩展性

公共数据授权运营可信环境应符合以下扩展性要求：

a) 应提供数据存储的扩容技术和方案，包括但不限于磁盘空间和数据库扩容技术；

b) 应支持根据业务量平滑扩展；

c) 系统应支持根据业务需求变化进行功能扩充；

d) 应按照 GB/T 37721 的功能要求，集成数据分析工具；

e) 应支持集成隐私计算技术，如联邦学习、多方安全计算等。

5.4 可维护性

公共数据授权运营可信环境应符合以下可维护性要求：

a) 应充分考虑系统软硬件及网络运行的实际情况，采用易于维护的系统平台；
b) 应用软件安装应简单友好且易于操作；
c) 系统软件配置应自动化，并规避复杂的系统配置文件；
d) 应支持系统管理员对 CPU、内存、硬盘可用空间、磁盘 I/O 等资源进行监控。

6 公共数据授权运营相关方及业务流程

6.1 流程概览

公共数据授权运营包括数据汇聚、数据授权、数据开发、数据交付四个主要阶段，见图 1。

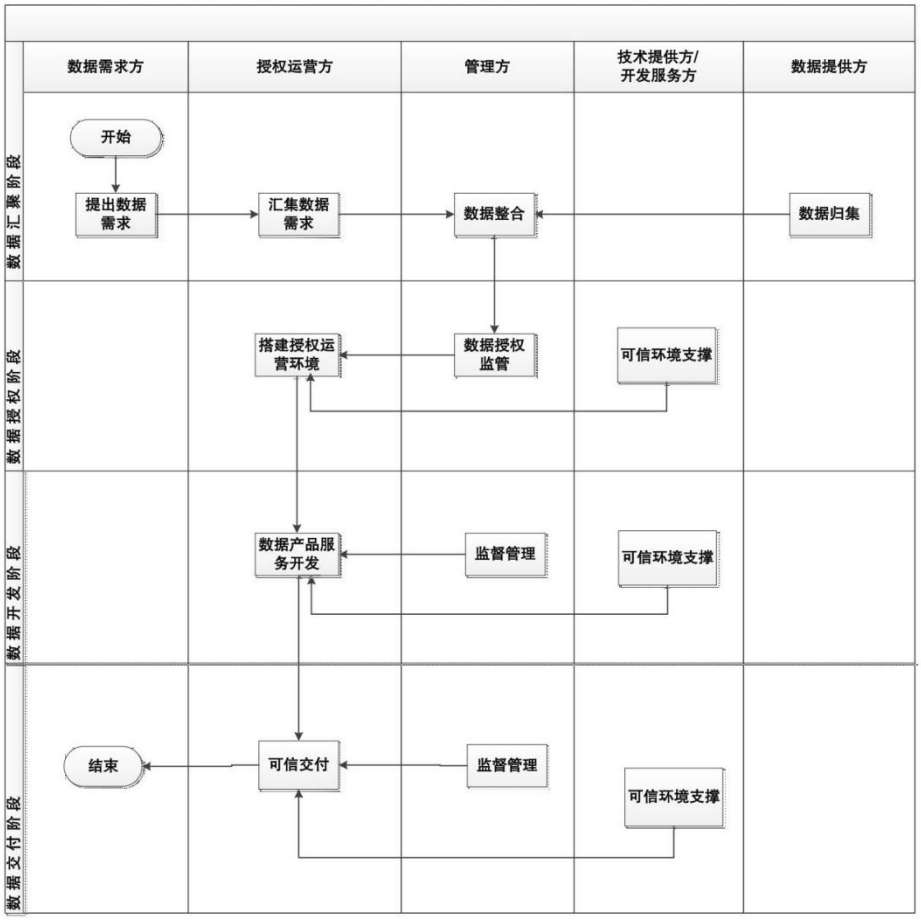

图 1 授权运营基本流程框架

6.2 数据汇聚阶段

数据汇聚阶段主要工作和要求如下：

a) 数据需求方通过授权运营方指定的渠道和平台提出公共数据需求；
b) 授权运营方接收、汇总、预审各需求方的数据需求，并发送给管理方；
c) 管理方对数据需求进行审核，基于浦东新区大数据资源平台匹配、整合数据资源；
d) 需求数据尚未归集到大数据资源平台的，管理方协同数据提供方归集相关数据。

6.3 数据授权阶段

数据授权阶段主要工作和要求如下：

a) 按照相关规定及协议，管理方对授权运营方提出的公共数据需求及目标应用场景进行授权，并对运营过程进行监督管理；
b) 授权运营方搭建安全可信环境，建立快捷的授权审批通道，对经授权的原始公共数据和公共数据产品做好信息登记。

6.4 数据开发阶段

数据开发阶段主要工作和要求如下：

a) 授权运营方在授权范围内，基于数据授权运营可信环境，实施数据开发利用，提供标准化、场景化的数据产品和数据服务，并对公共数据的数量、质量以及更新情况等进行实时监测和定期评估；
b) 管理方对授权运营方开发的公共数据产品和数据服务进行监管，按照 GB/T 37964 的安全要求，加强数据质量、数据安全问题发现及应急处置。

6.5 数据交付阶段

数据交付阶段主要工作和要求如下：

a) 授权运营方通过可信渠道和方式将公共数据产品和数据服务交付至数据需求方；
b) 授权运营方应充分了解需求并开展尽职审查，加强公共数据产品及服务交付的风险研判，异常情况及时向管理方上报；
c) 授权运营方应按照监管要求对其交付的公共数据产品和服务进行登记并可信存证。

6.6 相关方责任

公共数据授权运营主要相关方包括管理方、授权运营方、数据提供方、数据需求方、技术提供方、服务开发方。

6.6.1 管理方

管理方职责应包括但不限于：

a) 建立公共数据授权机制，健全相关管理制度和技术标准；
b) 遴选合适的授权运营方，对授权运营方遴选的技术提供方和服务开发方进行审核、监督；
c) 编制公共数据授权运营服务目录，制定计量计费标准；
d) 开展公共数据授权运营绩效评价工作，开展安全审计工作等。

6.6.2 授权运营方

授权运营方职责应包括但不限于：

a) 基于授权开展公共数据归集、治理、运营、流通、评估等相关工作；
b) 接受管理方委托遴选技术提供方和服务开发方，建设并安全运营公共数据授权运营平台；
c) 管理数据供给与需求，在可信环境中开展数据运营，按合同约定安全交付数据产品；
d) 管理数据运营相关的软硬件资产，开展市场拓展、场景授权、数据合约、安全监管等工作；
e) 动态监测、及时评估公共数据授权运营效能，对异常情况强化应急处置并及时报告管理方。

6.6.3 数据提供方

数据提供方职责应包括但不限于：

a) 对数据进行清洗、整理、加工等，强化数据分类分级及编目归集，保障数据准确性、完整性和可用性；
b) 建立健全数据质量控制体系，及时发现并解决数据质量问题，保障数据质量及更新的及时性。

6.6.4 数据需求方

数据需求方职责应包括但不限于：

a) 强化数据需求分析，明确数据种类、格式、质量、交付方式等要求，签署数据服务合同；
b) 按照合同约定时限，及时、准确接收数据，并对数据的准确性、完整性和可用性进行验收；
c) 按照合同约定用途，规范使用获取的数据产品及模型结果，确保数据安全，遵守保密义务。

6.6.5 技术提供方

技术提供方职责应包括但不限于：

a) 提供公共数据授权运营可信环境建设及运营所需的软、硬件产品支撑；
b) 提供各类安全查询、安全计算、安全交付等算法产品；
c) 提供软硬件产品升级迭代、运行维护等服务。

6.6.6 服务开发方

服务开发方职责应包括但不限于：

a) 接受授权运营方委托，基于技术服务方提供的软硬件产品及技术，搭建公共数据授权运营平台；强化平台的日常运营维护及数据运营行为的安全监测；
b）根据数据需求，接受授权运营方委托，开展多元数据融合、治理、交付、评估等运营服务。

7 公共数据授权运营可信环境总体架构

公共数据授权运营可信环境包含区块链、多方安全计算、联邦学习、可信执行环境和平台互联互通 5 个部分，见图 3。

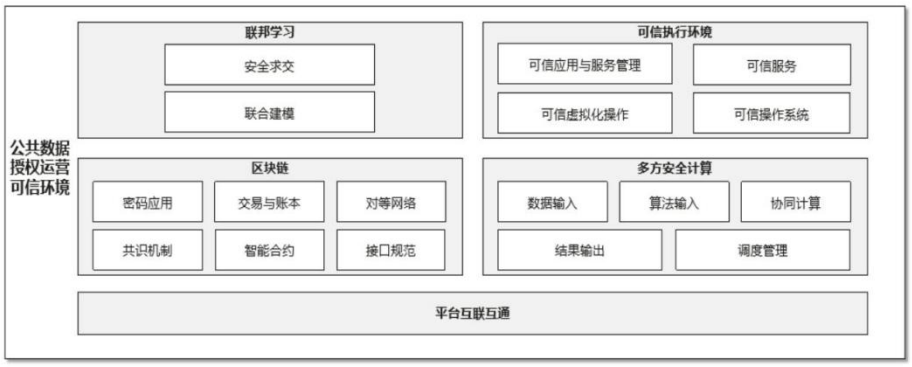

图 3 公共数据授权运营总体架构

7.1 区块链技术要求包括对密码应用、交易与账本、对等网络、共识机制、智能合约以及接口规范的要求；

7.2 多方安全计算技术要求包括对数据输入、算法输入、协同计算、结果输出、调度管理的要求；

7.3 联邦学习技术要求包括对安全求交、联合建模的要求；

7.4 可信执行环境技术要求包括对可信应用与服务管理、可信服务、可信虚拟化操作以及可信操作系统的要求；

7.5 平台互联互通包括保障区块链、多方安全计算、联邦学习等流程的互联互通。

8 公共数据授权运营可信环境技术要求

8.1 区块链

8.1.1 一般要求

a) 区块链技术全流程应用于公共数据授权运营的汇聚、授权、开发及交付环节；
b) 在汇聚环节，授权运营方借助密码应用、智能合约等技术进行区块链存证，通过数据目录上链及链上链下协同，保证数据提供方提供数据的不可篡改性；
c) 在授权环节，授权运营方将授权信息通过密码应用、共识机制、智能合约、对等网络等技术上传至区块链存证，保证授权信息不可篡改、可追溯；
d) 在开发环节，技术提供方和服务开发方的所有开发结果及过程信息都会在区块链存证，保障开发数据可追溯；
e) 在交付环节，授权运营方将交易信息上传至区块链存证，保证交付信息的可追溯性，并制定相应的接口规范，保证不同区块链之间数据的互通性。

8.1.2 密码应用

密码应用具备要求如下：

a) 应符合密码相关国家标准、行业标准的有关要求；
b) 使用的密码技术应遵循相关国家标准和行业标准；
c) 使用密码产品与密码模块应通过国家密码管理部门核准；
d) 使用的密码服务应通过国家密码管理部门许可。

8.1.3 共识机制

共识机制具备要求如下：

a) 应具备符合业务需求的容错性，包括节点物理或网络故障的非恶意错误、节点遭受非法控制的恶意错误以及节点产生不确定行为的不可控错误等；
b) 应能满足应用场景的一致性要求，应具备满足业务需求的收敛速度和确认时间；
c) 宜具备分叉管理能力，具备防止分叉导致的安全问题；
d) 应保证公平，不存在后门以避免特殊人员为了特殊目的干扰共识机制的达成逻辑，从而形成有利于特定人员的共识结论。

8.1.4 交易与账本

交易与账本具备要求如下：

a) 应支持持久化存证记录；
b) 支持多节点拥有完整的数据记录；
c) 支持向获得授权者提供真实的数据记录；
d) 确保有相同数据记录的各节点的数据一致性；
e) 行为或数据需记录相应的一致性的时序，并具备时序容错性。

8.1.5 智能合约

智能合约具体要求如下：

a) 应具备防篡改和抗抵赖性；
b) 在编程语言选择上，宜采用最新的稳定版本；
c) 合约代码应符合书写规范、逻辑要求等规范性要求；
d) 应具备生命周期管理，包括合约的创建、部署、升级、触发、执行、废止等；
e) 宜具备应急响应机制，可在发现合约漏洞后，及时检查和修复。

8.1.6 对等网络

对等网络具体要求如下：

a) P2P 通信过程宜采用本地的、自主的、双向的认证和授权；
b) 应将数据的传输限制在特定授权节点间，确保数据和信息在传输过程中不被非授权用户读取和篡改。

8.1.7 接口规范

接口规范具体要求如下：

a) 应遵循最小化原则，对相关方公开的接口应将其能进行的操作最小化；
b) 宜对接口访问权限进行等级划分，针对不同用户配置不同的访问权限。

8.2 多方安全计算

8.2.1 一般要求

a) 多方安全计算技术一般应用于公共数据授权运营的开发环节；
b) 在开发环节，授权运营方、技术提供方和服务开发方应借助多方安全计算的数据输入、算法输入、协同计算、结果输出、调度管理等技术保证参与各方仅可获得己方计算结果，无法推测出其他方的输入数据。

8.2.2 数据输入

授权运营方数据输入具体要求如下：

a) 数据运营方应将隐私数据转化为输入因子，提供给指定计算节点，并确保在设定的安全模型下无法通过输入因子推算出输入数据；

b) 数据运营方应对数据源、数据集、元数据进行统一管理；

1）数据源管理：

——应支持不同类型的数据源接入，包括但不限于数据库和文件，数据库类型如关系型数据库、列式数据库、数据仓库等；

——可扩展支持新的数据类型。

2）数据集管理：

——应支持对数据集的添加、删除操作；

——应支持数据集接入状态查询功能，展示所有数据集接入任务的状态；

——应支持监控数据集参与计算状态的功能，如正在参与计算、使用完毕等。

3）元数据管理：

——应支持使用元数据描述数据集；

——应支持元数据查询功能，包括名称、标记、描述、大小、样例、类型等信息。

c) 应具备数据存储格式转换、数据预处理等功能；

d) 应对发送数据进行存证。

8.2.3 算法输入

算法输入提供对算法逻辑的管理，具体要求如下：

a) 应支持常见的查询操作，如 Select、Sort、Join 等；

b) 应支持常见的统计分析算法，如均值、方差、中位数等；

c) 应支持常见的机器学习算法，如线性回归、逻辑回归、神经网络、决策树等。

8.2.4 协同计算

应由多个计算节点组成多方安全计算引擎，协同实现多方安全计算协议，具体要求如下：

a) 基础运算：

1）应支持加、乘、比较等基础运算；

2）应支持与、或、非等逻辑运算；

3）应支持整数、小数、常见字符、字符串在内的一种或多种基本数据类型。

b) 多方安全计算节点：

1）应能根据数据运营方提供的输入因子，匹配算法逻辑并执行计算任务；

2）应保证直接在计算因子上完成运算，得到输出因子；

3）应能清除计算过程缓存的计算因子；

4）应能并发处理不同的计算任务；

5）应能将输出因子发送给数据运营方进行解析。

8.2.5 结果输出

结果输出的具体要求如下：

a) 应能接受计算方法输出因子；

b) 应对接受数据进行存证；

c) 应保证输出结果的正确性。

8.2.6 调度管理

调度管理的具体要求如下：

a) 应对多方安全计算的参与方进行管理；
b) 应支持与用户交互创建任务，生成任务配置信息；
c) 应能将具体任务配置信息分发给数据提供方、授权运营方、数据需求方；
d) 应对多任务执行进行统一调度，包括任务排队、负载以及优先级调度等；
e) 应能监控、管理任务执行过程；
f) 应保存任务执行结果等；
g) 宜支持基于计算节点动态发现、任务动态分配。

8.3 联邦学习

8.3.1 一般要求

a) 联邦学习技术一般应用于公共数据授权运营的开发环节；
b) 在开发环节，授权运营方、技术提供方和服务开发方应借助联邦学习的安全求交、联合建模等技术实现分布式计算，保证参与方的数据隐私，防止敏感信息泄露。

8.3.2 安全求交

安全求交的具体要求如下：

a) 基于哈希算法、国际密码、国密等密码的多种安全求交算法能力；
b) 应提供对两方或两方以上数据进行安全求交的能力，宜提供基于时间等多种复合条件的安全求交能力；
c) 宜支持在安全求交的同时对结果进行加工处理。

8.3.3 联合建模

联合建模的具体要求如下：

a) 应提供横向联邦学习、纵向联邦学习两类联邦学习算法能力；
b) 应提供多种建模处理能力，包括：
   1) 联邦化的数据清洗、特征分箱、特征编码、特征变换、特征选择等特征工程；
   2) 支持常见的算法开发框架等用于监督、非监督等机器学习或深度学习算法的开发；
   3) 支持机器学习模型的多种评价指标计算；
   4) 支持模型在线、离线推理和批量推理；
c) 应采用同态加密、多方安全计算、差分隐私、可信硬件等安全技术保护中间数据，防止从中间数据逆推出原始数据及隐私参数。

8.4 可信执行环境

8.4.1 一般要求

a) 可信执行环境一般应包含可信虚拟化系统、可信操作系统、可信服务等技术，应用于公共数据授权运营的汇聚、授权、开发、交付环节；
b) 在汇聚环节，授权运营方、技术提供方和数据提供方应借助可信执行环境相关技术，保证参与方汇聚数据的隐私；

c) 在授权环节，授权运营方、技术提供方和数据提供方应借助可信执行环境相关技术，保证参与方授权环节的隐私；
d) 在开发环节，授权运营方、技术提供方和服务开发方应借助可信执行环境相关技术，实现多方安全计算和联邦学习，保证参与方的数据隐私，防止敏感信息泄露；
e) 在交付环节，授权运营方、技术提供方和服务开发方应借助可信执行环境相关技术，保证参与方的交付数据隐私。

8.4.2 可信虚拟化系统

可信虚拟化系统具备要求如下：
a) 应具备创建、删除等动态管理可信执行环境内虚拟机的能力；
b) 应具备管理可信执行环境中虚拟机内部 CPU、内存、外设等硬件资源的能力；
c) 可信执行环境内虚拟机之间应具备互相通信和数据交换的能力。

8.4.3 可信操作系统

可信操作系统具体要求如下：
a) 应保证可信应用及可信服务仅根据其所分配的权限访问相应的资源，不能越权访问；
b) 应保证系统自身、可信服务能够正确、完整地加载启动及代码执行；
c) 应具备可信应用之间、可信应用与可信服务之间的访问控制能力；
d) 对于系统权限的管理，应避免将应用最高权限赋予可信服务，当某个可信服务出现异常时，不影响系统内核及其他可信应用及服务的正常工作。

8.4.4 可信应用与服务管理

可信操作系统具体要求如下：
a) 对可信应用及服务的管理，宜采用设备厂商提供的根证书、应用发布证书来进行认证，以确保应用数据的机密性、完整性、真实性和行为的不可否认性；
b) 当可信应用部署到可信执行环境时，可信执行环境应校验可信应用的真实性和完整性，并根据可信应用供应商所拥有的权限，对其资源访问及通信范围等进行严格控制。

8.4.5 可信服务

可信服务具体要求如下：
a) 可信服务宜包括可信时间服务、可信加解密服务、可信存储服务、可信身份鉴别服务、可信设备鉴证服务等；
b) 可信加解密服务应保证仅获得相应授权的可信应用或可信服务才可以访问密钥；
c) 可信存储服务应具备访问控制机制，确保只有授权的应用才能访问相应的存储空间；
d) 可信存储应提供对于数据回滚攻击的防御措施；
e) 可信身份鉴别服务应能通过识别用户个人身份数字特征信息来识别用户身份及权属；
f) 可信设备鉴证服务应能检测可信执行环境运行的健康状态。

8.5 平台互联互通

平台互联互通应保障流程的互联互通，具体要求如下：
a) 应支持标准化作业流程，包括创建作业、数据加载、作业执行与调度、任务执行与调度、模型加载与管理等；
b) 应支持描述作业及任务调度的通信、计算、存储资源的标准接口，确保算法的可移植性；

c) 应提供标准可运行的算法镜像以及镜像运行必要的信息，包括名称、版本、必要的目录结构与参数信息等。

8.6 公共数据授权运营监管管理

8.6.1 一般要求

数据汇聚阶段的监督具体要求如下：

a) 公共数据授权运营监督管理分为两类：管理方监督授权运营方、数据提供方和数据需求方的授权运营活动；授权运营方监督技术提供方和服务开发方的授权运营活动；
b) 管理方监督，包括监督数据提供方在数据汇聚阶段的活动，监督授权运营方在数据授权、数据开发、数据交付阶段的活动，以及监督数据需求方在数据交付后的数据使用活动等，是否符合可信、隐私、安全等要求；
c) 授权运营方应监督技术提供方和服务开发方在数据授权、开发、交付阶段的活动是否符合可信、隐私、安全等要求。

8.6.2 数据汇聚阶段监管要求

数据汇聚阶段的监督具体要求如下：

a) 管理方应设计完善的公共数据汇聚规则；
b) 授权运营方应设计完善的数据汇聚监测制度和监测计划；
c) 授权运营方应借助区块链技术对数据汇聚全流程的数据进行监测并存证；
d) 授权运营方应支持对汇聚阶段的用户行为、账户权限、日志、算法等进行审计。

8.6.3 数据授权阶段监管要求

数据授权阶段的监督具体要求如下：

a) 管理方应设计完善的公共数据授权规则；
b) 授权运营方应设计完善的数据授权监测制度、监测计划、预警制度；
c) 授权运营方应借助区块链技术对数据授权全流程的数据进行监测并存证；
d) 授权运营方应支持对授权阶段的用户行为、账户权限、日志、算法等进行审计。

8.6.4 数据开发阶段监管要求

数据开发阶段的监督具体要求如下：

a) 管理方应设计完善的公共数据开发规则；
b) 授权运营方应设计完善的数据开发监测制度、监测计划、预警制度及应急措施；
c) 授权运营方应借助区块链技术对数据开发全流程的数据进行监测并存证；
d) 授权运营方应支持对开发阶段的用户行为、账户权限、日志、算法等进行审计。

8.6.5 数据交付阶段监管要求

数据交付阶段的监督具体要求如下：

a) 管理方应设计完善的公共数据交付规则；
b) 授权运营方应设计完善的数据交付监测制度和监测计划；
c) 授权运营方应借助区块链技术对数据交付全流程的数据进行监测并存证；
d) 授权运营方应支持对交付阶段的用户行为、账户权限、日志、算法等进行审计。

9 应用场景

通过建立可信环境，推进公共数据授权运营，提高公共数据社会化开发利用水平，典型应用场景见附录A。

附 录 A
（资料性）
公共数据授权运营可信环境典型应用场景

表 A.1 典型应用场景

序号	应用分类	典型场景	场景描述
1	治理数字化	群租房管理	通过各种数据来源（包括水、电、煤、气、不动产、人口等），获取实有人口、房型、建筑面积、用电量、用水量、用气量、外卖、快递等静态或实时数据，进行清洗、融合、存储及建模后得出分析结果。模型有三种：实有人口模型、水电气模型、外卖快递模型。根据模型设定认定为疑似群租的，进入网格派单系统流转，由执法人员上门检查，确认后责令整改或依法处理。
2	生活数字化	智慧保险	智慧保险需要可信环境中开展多元数据融合分析，实现在不泄露原始数据、保护用户隐私的前提下挖掘数据价值，用于车辆核保、中小企业信用保证险、电梯保险、骑手保险等保险创新业务。
3	经济数字化	“AI”+创新药	“AI+”创新药借助隐私计算技术，可以在保护健康医疗敏感数据不出域前提下，将药企的算法模型部署到可信环境中，在“双盲”的情况下，打破健康医疗数据共享的难题，实现健康医疗数据的价值输出。
4		临床试验受试者匹配	利用多方安全计算等技术，链接数据提供方和数据使用方，在“数据不出域，可用不可见”的可信环境下，将多个医院的病理系统、HIS 系统、LIS 系统等多平台数据融合分析，帮助药企解决受试者招募难题，快速实时地发现新鲜病例，进而加快临床试验进程，节约临床试验成本。
5		市场精准营销	企业利用区块链、多方安全计算、联邦学习等技术，借助支付、社交应用等多方数据，丰富用户特征维度，构建用户模型，以实现目标用户挖掘与用户意向的精准触达，实现精准营销或交叉销售。
6		金融风控精准招商	利用区块链、多方安全计算、联邦学习等技术，在确保银行和政府两方数据不出各自域的基础上，应用于小微企业普惠金融业务，构建全面的企业信用画像，辅助提升授信业务贷款审批工作效率，助力银行提升风控水平，解决中小企业融资难问题，安全高效服务实体经济。并可构建企业信用评价模型，推动政务数据与金融数据互通，助力企业融资、辅助政府智慧招商，助力区域经济发展。

参考文献

[1]《政务信息系统整合共享实施方案》(国办发〔2017〕39号)
[2]《国务院关于加快推进全国一体化在线政务服务平台建设的指导意见》(国发〔2018〕27号)
[3]《进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案》(国办发〔2018〕45号)
[4]《上海市公共数据和一网通办管理办法》(沪府令〔2018〕9号)
[5]《上海市加快推进数据治理促进公共数据应用实施方案》(沪委办〔2019〕8号)
[6]《2020年上海市深化“一网通办”改革工作要点》(沪委办〔2020〕12号)
[7]《上海市政务信息系统整合实施方案》(沪经信推〔2019〕231号)
[8]《可信区块链：安全评估指标与测试方法》可信区块链推进计划团体标准
[9]《可信区块链标准：第3部分 评测方法》可信区块链推进计划团体标准
[10]JR/T 0184–2020 金融分布式账本技术安全规范
[11JR/T 0193–2020 区块链技术金融应用 评估规则
[12]YD/T 3747–2020 区块链技术架构安全要求
[13]T/PCAC 0009–2021 多方安全计算金融应用评估规范
[14]GB/T 41388–2022 信息安全技术 可信执行环境 基本安全规范
[15]Blockchain and distributed ledger technologies — Reference architecture, ISO CD 23257

上海市浦东新区市场监督管理局办公室　　2023年12月15日印发