**《隐私计算 可信数据服务平台框架、功能及接口》编制说明**

1. **编制的目的和意义**

2022 年10 月，党的二十大报告明确提出了要加快建设数字中国。数据作为数字中国建设的新型生产要素和关键战略性资源，需要流通共享才能更好地发挥价值。然而，数据流通共享将导致数据安全形势更为严峻，严重威胁个人隐私、商业秘密、国家机密。以联邦学习、多方安全计算、可信执行环境为代表的隐私计算是实现数据流通共享过程中可用不可见的重要技术，备受学界业界关注。近年来隐私计算取得了重要进展，但在高性能、高安全、技术融合、跨平台应用等方面仍然面临诸多挑战。为加快隐私计算基础理论和关键技术的研究、可信数据服务平台的搭建，需尽快推进隐私计算标准化建设，做好顶层设计工作，对保障数据安全流通和发挥数据资源价值具有重要意义。

（一）政策依据

为贯彻落实《关于构建更加完善的要素市场化配置体制机制的意见》、《关于构建数据基础制度更好发挥数据要素作用的意见》（数据二十条）、《数据安全法》、《个人信息保护法》、《数字中国建设整体布局规划》、《关于促进数据安全产业发展的指导意见》、《中国区块链创新应用发展报告（2023）》、《区块链和分布式记账技术标准体系建设指南（2024）》、《重庆市数字经济“十四五”发展规划（2021—2025 年）》等文件要求，结合实际需求，制定符合行业现状的《隐私计算 可信数据服务平台框架、功能及接口》。

（二）研究背景

2022 年10 月，党的二十大报告明确提出了要加快建设数字中国。2023 年2 月，中共中央、国务院联合印发了《数字中国建设整体布局规划》，指出加快数字中国建设对全面建设社会主义现代化国家、全面推进中华民族伟大复兴具有重要意义和深远影响。而这其中，数据作为基础战略性资源，是数字中国建设的基石。

2020 年4 月，中共中央、国务院颁布了《关于构建更加完善的要素市场化配置体制机制的意见》，首次明确将数据作为新型生产要素。数字中国建设亟需充分释放数据要素价值，而作为释放数据要素价值的关键环节，数据资源的开放、共享和流通的需求日益强烈。2022 年12 月，中共中央、国务院印发的《关于构建数据基础制度更好发挥数据要素作用的意见》（数据二十条）提出，数据合规高效流通要以维护国家数据安全、保护个人信息和商业秘密为前提。如何在保障数据安全的前提下充分发挥数据价值，是当前亟待解决的重要问题。以联邦学习、多方安全计算、可信执行环境（Trusted Execution Environment， TEE）为代表的隐私计算是实现数据在流通共享过程中可用不可见的重要技术.

前期经过调研，了解到我市各县区 (市) 的基于隐私计算技术构建数据可信流通环境正处于初步阶段，没有统一的系统框架和基础标准，还没有成为一个闭合的体系。如何平衡数据安全与数据共享流通需进一步的梳理逻辑关系，急需理顺各自的需求及责任范围。

（三）可行性分析

我国一方面高度重视保护数据安全和个人隐私,相继实施《数据安全法》和《个人隐私保护法》；另一方面，高度重视促进数据共享和流通，充分释放数据要素价值。作为平衡数据安全和数据共享流通矛盾的关键核心，我国隐私计算技术及应用快速发展，得到了政府的大力支持和投入。2021 年5 月，发改委牵头联合印发《全国一体化大数据中心协同创新体系算力枢纽实施方案》，提出试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式，构建数据可信流通环境，提高数据流通效率。2023 年1 月，工信部、网信办、发改委等十六部门印发《关于促进数据安全产业发展的指导意见》，提出加强隐私计算、数据流转分析等关键技术攻关。根据当前趋势，制定《隐私计算 可信数据服务平台框架、功能及接口》团体标准，以确保基于隐私计算技术构建数据可信流通环境标准的一致性和适用性。最终支持隐私计算可信数据服务平台的搭建与业务扩展。所以制定《隐私计算 可信数据服务平台框架、功能及接口》团体标准是有必要的。

1. **编制原则和依据**

本标准的制定工作遵循“面向市场、服务产业、自主制定、适时推出、及时修订、不断完善”的原则，本着先进性、科学性、合理性和可操作性的原则，结合隐私计算及可信数据流通环境发展实际，按照 GB/T1.1— 2020 给出的规则编写。

1. **编制过程**

（一）主要起草单位、起草人和协作起草单位

本标准由重庆市科学技术研究院作为主要起草单位，编制《隐私计算 可信数据服务平台框架、功能及接口》标准，广泛邀请相关行业单位参与编制工作，计划项目完成时间是2025年6月。

（二）标准起草工作过程

为了确保标准编制的顺利实施，做到编制的标准技术含量高、实用性强，确保编制标准高质量、高效率。标准起草单位成立了标准起草小组，负责调研、标准的编制、修改、送审等工作的实施。

标准起草工作组成员组织认真学习了 GB/T1.1— 2020《标准化工作导则第 1 部分：标准的结构和 编写规则》，结合标准制定工作程序的各个环节，进行了探讨和研究。收集了隐私计算及可信数据流通环境相关的国家/地方/行业标准资料，并参考学习了这些资料，形成了《隐私计算 可信数据服务平台框架、功能及接口》草案。同时，起草小组组织了相关专家及技术人员对标准草案进行了多次讨论，根据讨论结果，对标准草案中的部分内容做了多次修改完善，形成了本标准送审稿。

1. **技术性说明**
2. 制定标准的原则和依据，与有关现行国际国内标准的关系

本标准在编制的过程中，从生产实际出发，参考其他相关的标准，以提高标准的准确性，以科学性和实用性为原则。同时，遵循国家的有关方针、政策、法规，按照GB/T 1.1-2020《标准化工作导则 第一部分：标准化文件的结构和起草规则》进行编制，力求做到技术内容正确无误；文字表达准确、简明易懂；标准结构严谨合理；层次划分符合逻辑。本标准主要规定了基于隐私计算技术构建可信数据服务平台的框架、功能及接口规则。

本标准引用了GB/T 25069-2022《信息安全技术 术语》、GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 32908-2016《非结构化数据访问接口规范》、GB/T 35295-2017《信息技术 大数据 术语》、GB/T 32905-2016《信息安全技术 SM3密码杂凑算法》、GB/T 32907-2016《信息安全技术 SM4分组密码算法》、GB/T 32918-2016《信息安全技术 SM2椭圆曲线公钥密码法》、GB/T 35275-2017《信息安全技术 SM2密码算法加密签名消息语法规则》、GB/T 35276-2017《信息安全技术 SM2密码算法使用规范》、GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、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》12个标准。

1. 主要条款说明

本标准主要技术内容拟包括：范围、规范性引用文件、术语定义、隐私计算技术、可信执行环境。具体如下：

1.范围

本标准规定了隐私计算可信数据服务平台的参考框架及其组成，具体包括平台框架、平台功能和接口规范。本标准适用于基于隐私计算的可信数据服务平台的研发、测试、评估和验收等。

2.规范性引用文件

本标准依据 GB/T 1.1-2000 《标准化工作导则第 1 部分：标准的结构和编写规则》、GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 32908-2016《非结构化数据访问接口规范》、GB/T 35295-2017《信息技术 大数据 术语》、GB/T 32905-2016《信息安全技术 SM3密码杂凑算法》、GB/T 32907-2016《信息安全技术 SM4分组密码算法》、GB/T 32918-2016《信息安全技术 SM2椭圆曲线公钥密码法》、GB/T 35275-2017《信息安全技术 SM2密码算法加密签名消息语法规则》、GB/T 35276-2017《信息安全技术 SM2密码算法使用规范》、GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、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》要求进行编写。

3.术语和定义

主要对隐私计算技术及可信数据执行环境进行了定义。

4.隐私计算技术

隐私计算技术主要规定了以联邦学习、多方安全计算、可信执行环境（Trusted Execution Environment，TEE）为代表的隐私计算技术。

5.可信执行环境

主要对平台里面涉及到的有关可信执行环境进行了规定。

1. **采标情况**

没有采用国际标准和国外先进标准。

1. **重大意见分歧的处理**

无。

1. **标准实施的建议**

标准发布后，建议在协会内加强培训和宣贯力度，组织相关单位以本标准为依据牵头进行平台建设，落实标准中的相关要求。促使隐私计算可信数据服务平台规范化、标准化，保障数据安全的前提下充分发挥数据价值。

1. **其他应予说明的事项**

无。

《隐私计算 可信数据服务平台框架、功能及接口》标准起草小组

2025年4月1日