ICS 03.060
CCS A11

T/GDXY

团 体 标 准

T/GDXY 003—2026

普惠金融数字信用服务 可信数据交互空间建设要求

Digital inclusive financial services - Construction requirements for trusted data interactive space

（征求意见稿）

2026－XX－XX 发布 2026－XX－XX 实施

广东省信用协会 发 布

目　　次

前　言

普惠金融数字信用服务系列标准构成“基础支撑—核心能力—生产规范—风险管理—人才保障”完整闭环体系，T/GDXY 0003—2026《普惠金融数字信用服务　可信数据交互空间建设要求》是普惠金融数字信用服务系列标准之一，为信用服务提供基础支撑。本系列标准结构如下：

——T/GDXY 0003—2026 普惠金融数字信用服务 可信数据交互空间建设要求；

——T/GDXY 0004—2026 普惠金融数字信用服务 信用评价模型；

——T/GDXY 0005—2026 普惠金融数字信用服务 数字要素驱动信用生产规范；

——T/GDXY 0006—2026 普惠金融数字信用服务 动态风险管理；

——T/GDXY 0007—2026 普惠金融数字信用服务 村级普惠金融服务人员能力要求。

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。

本文件由茂名市财政局提出。

本文件由广东省信用协会归口。

本文件起草单位：茂名市财政局、中国工商银行、中国建设银行、中国邮政储蓄银行、中国农业银行、广发银行、广东顺德农商银行、中国太平洋保险(集团)股份有限公司、广东惠龙邦数字科技有限公司。

本文件主要起草人：梁极。

普惠金融数字信用服务 可信数据交互空间建设要求

1 范围

本文件规定了普惠金融数字授信服务可信数据交互空间的总体架构、服务平台要求、连接器要求、数据资源管理要求、信用产品特征要求、安全技术要求、运行维护要求。

本文件适用于普惠金融相关机构或组织开展数字授信服务可信数据交互空间建设的规划、建设、运营和管理。

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。

TC609-6-2025-01 可信数据空间 技术架构

TC609-6-2025-14 可信数据空间 数字合约技术要求

TC609-6-2025-15 可信数据空间 使用控制技术要求

TC609-6-2025-16 可信数据空间 技术能力评价规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字普惠金融 digital inclusive finance

运用数字技术为三农、小微、低收入群体等提供可得、便捷、安全的信贷、征信、支付等金融服务。

3.2

可信数据空间 trusted data space

基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。

3.3

可信数据交互空间 trusted data interactive space

在普惠金融数字授信服务场景下，遵循国家“可信数据空间”技术架构要求，以政务数据为权威基座，连接政府、金融机构、产业主体等多方主体，依托共识规则、隐私计算、区块链、可信执行环境等技术，在数据不出域、可用不可见、可控可溯源前提下，实现多源数据安全交互、跨域融合、可信流通、信用建模、数字授信支撑的数据共享基础设施与协同治理空间。

注1：本文件中的“可信数据交互空间”是“可信数据空间”在普惠金融数字授信服务领域的行业化应用与具体体现。

注2：其通用技术架构应符合TC609-6-2025-01的要求。

3.4

可信数据空间服务平台 trusted data space service platform

可信数据空间的核心管理枢纽，具备身份管理、连接器管理、目录管理、合约管理、可信数据空间管理、数据使用控制等核心功能。

[来源：TC609-6-2025-01]

3.5

可信数据空间连接器 trusted data space connector

多方主体参与可信数据空间生态的入口系统，支持数据提供方、数据使用方、数据服务方通过连接器提供数据、使用数据以及提供增值服务。

[来源：TC609-6-2025-01]

3.6

使用控制 usage control

依托动态策略引擎，对数据使用者的身份、行为、环境等多维度属性开展实时评估，进而实现对数据访问、分析、计算及处理等行为进行精细化管控的技术。

3.7

数字授信服务 digital credit service

以数据为驱动、以技术为手段，通过分析多源信用信息对借款人进行信用评估、风险定价和授信决策的金融服务模式。

4 缩略语

下列缩略语适用于此文件：

API：应用程序编程接口（Application Programming Interface）

CA：证书认证机构（Certificate Authority）

5 总体架构

5.1 通用架构

普惠金融数字授信服务可信数据交互空间的技术架构应符合TC609-6-2025-01的要求，由可信数据空间服务平台和可信数据空间连接器两大核心组件构成。服务平台负责空间的可信管理与服务输出，连接器负责多源数据的合规接入与数据交付。

5.2 参与角色

可信数据交互空间涉及的参与角色及其职责应符合表2的规定。

表1 可信数据交互空间相关角色及职责

角色	职责
数据提供方	提供政务数据、产业数据、金融数据等，通过连接器接入空间
数据使用方	主要为银行、保险等金融机构，通过连接器使用信用服务产品
数据服务方	提供数据开发、隐私计算、模型训练等增值服务
空间运营方	负责服务平台的运营管理、接入审核、规则制定
监管方	政府或金融监管部门，监督合规运行

6 可信数据空间服务平台要求

6.1 身份管理

服务平台应具备统一身份管理能力。具体要求如下：

a) 应对接入主体（数据提供方、数据使用方、数据服务方）的身份进行统一管理和验证；

b) 应对接入连接器的身份进行认证、更新、注销等全生命周期管理；

c) 应引入国家网络身份认证、CA 数字证书体系等符合国家要求的身份认证机制；

6.2 连接器管理

服务平台应具备连接器管理能力，具体要求如下：

a) 应支持接入连接器的注册、认证、运行监测、能力适配和注销等全生命周期管理；

b) 应支持对接入连接器的运行状态进行持续监测和健康检查；

c) 宜支持对接入连接器进行远程配置和升级管理。

6.3 目录管理

服务平台应具备统一目录管理能力。具体要求如下：

a) 应支持数据产品和数据资源的统一登记，提供标准化的登记接口，代数据提供方或数据服务方完成数据产品和数据资源的登记、更新和撤销；

b） 应建立统一的数据目录体系，支持数据产品和数据资源的发布、发现与检索；
c） 应支持数据产品目录管理，提供数据产品上架、分类标签、下架等管理功能；
d） 宜支持数据使用方申请订阅数据产品；
e） 应支持按普惠金融场景、对象建立主题目录；
f） 目录信息应包括数据来源、更新频率、质量评分、访问权限等元数据。

6.4 合约管理

服务平台应具备合约管理能力。具体要求如下：
a） 应支持合约的全生命周期管理，包括合约创建、协商签署、备案存证、履行执行、终止解除等环节；
b） 合约内容应包括合约标识、签署主体、合约标的、合约策略、有效期、签署签名等要素；
c） 应支持服务平台作为中介方协调多方主体达成共识签署等签署模式；
d） 应支持合约策略的定义与执行，合约策略应覆盖使用者（Who）、使用时间（When）、使用环境（Where）、数据内容（What）、使用方式（How）、使用次数（How Much）等控制维度；
e） 应使用机器可解释的标记语言（如 XML、JSON 等格式）对合约内容进行描述，确保合约可被策略执行节点识别和执行；
f） 应符合 TC609-6-2025-14 的规定。

6.5 数据使用控制

服务平台应具备数据使用控制能力。具体要求如下：
a） 应集成隐私保护计算、数据沙箱、数据匿名化等技术，提供安全的数据使用环境；
b） 应与数据使用环境联动，对数据使用行为进行实时监测与控制，确保数据使用符合合约要求；
c） 应对数据使用过程进行细粒度存证，支持日志查询与溯源；
d） 应符合 TC609-6-2025-15 的规定；
e） 应遵循最小必要原则，对数据访问和计算请求进行严格审核，确保其限于特定场景且为最小化必需；
注：最小必要原则：处理个人信息应当具有明确、合理的目的，应当与处理目的直接相关，采取对个人权益影响最小的方式；收集个人信息应当限于实现处理目的的最小范围，不得过度收集个人信息。
f） 控制粒度宜达到字段级，在普惠金融授信场景中应支持对信用评分、信用报告等数据产品中涉及个人敏感信息的字段进行精细化管控。

6.6 扩展功能

服务平台应按需建设以下扩展功能：
a） 数据开发：支持多方联合建模、联邦学习等数据开发利用能力；
b） 数据产品化：支持将信用评分、信用报告等输出物封装为标准化数据产品；
注：具体产品形态可包括信用评分（如“农信分”）、信用报告（如“农信报告”）、动态白名单等。
c） 价值分配：建立按调用量或价值贡献分级计费的流通计价机制。

7 可信数据空间连接器要求

7.1 数据交付

连接器应支持安全、可靠的数据传输与交付机制。具体要求如下：
a） 应支持端到端加密传输；
b） 应支持断点续传和数据完整性校验。

7.2 数据资源管理

连接器应支持本地数据资源管理。具体要求如下：
a） 应对接入的本地数据资源进行编目、存储和管理；
b） 宜支持数据资源的版本管理和更新同步。

7.3 数据产品管理

连接器应支持数据产品管理。具体要求如下：

a) 宜支持将数据资源转化为标准化数据产品；

b) 宜支持数据产品的发布、订阅和交付。

7.4 合约管理

连接器应在侧执行合约策略。具体要求如下：

a) 应接收并执行服务平台下发的合约；

b) 应在数据使用前验证合约的有效性和授权范围。

7.5 数据使用控制

连接器应实时执行使用控制策略。具体要求如下：

a) 应在数据被使用的瞬间进行实时校验与控制；

b) 应记录使用行为日志，支持审计追溯。

7.6 部署形态

连接器应支持多种部署形态。具体要求如下：

a) 软件连接器：支持在标准服务器上部署的纯软件形态；

b) 边缘节点：宜部署轻量边缘节点，支撑遥感解译、物联网数据预处理、低时延授信。

8 数据资源管理要求

8.1 数据分类

可信数据交互空间应汇聚普惠金融核心数据，具体分类及内容应符合表3的规定。

表2 普惠金融数据分类

数据类别	数据内容
基座政务数据	工商、税务、土地确权、补贴、不动产、资质许可、行政处罚、农业农村、自然资源等
征信数据	央行征信、持牌市场化征信机构数据，覆盖负债、逾期、担保、司法失信
产业数据	卫星遥感、农机物联网、养殖环境、作物长势、种养备案、产能产值、供应链交易、价格波动
商业数据	电商流水、农业保险、物流、支付结算、经营履约数据
主体数据	农户、新型农业经营主体、小微企业、个体工商户、产业职工基础信息
气象时序数据	降水、温度、灾害天气、季节气候，支撑产能评估与风险预警

8.2 数据质量要求

8.2.1 应对接入数据的质量进行校验和持续监测，建立数据质量管控机制。

8.2.2 应建立数据质量评估标准，对不满足质量要求的数据，应建立自动熔断、拦截、告警和回溯修正机制。

8.2.3 各数据源应统一更新频率和口径，确保数据时效性，适配动态信用评价需求。

8.3 授权合规要求

8.3.1 授权应符合授权主体、目的、范围、期限四要素的要求，且应明示同意、遵循最小必要原则。

8.3.2 应支持授权、撤回、查询、更正、删除，且应实现日志留痕、全链路可追溯。

8.3.3 不应超范围、超期限或未经授权使用数据，不应转存、复用或泄露原始数据。

9 信用服务产品特征要求

9.1 通用要求

服务平台应具备将多源数据转化为标准化信用服务产品的能力。

信用服务产品的输出应以“原始数据不出域、可用不可见”为原则，输出的应是信用评分、信用报告、风险标签、动态白名单、授信建议等价值结论，不应输出原始数据。

9.2 信用服务产品类型

服务平台应支持输出表4所列类型的信用服务产品。

表3 信用服务产品类型

序号	产品类型	产品描述
1	信用评分	基于多维度信用信息综合计算得出的量化分值，反映主体的信用状况和风险水平。
2	信用报告	结构化、可视化、可审计的信用信息汇总文档，包含主体的信用画像、评价维度得分、风险提示等内容
3	风险标签	对主体特定风险特征的标识性描述，例如“高负债风险”“经营波动风险”“涉诉风险”等
4	动态白名单	基于实时数据自动生成和更新的合格客群名单
5	授信建议	基于信用评估结果输出的授信额度、利率、期限等授信方案建议

10 安全管理要求

10.1 总体要求

应建立覆盖数据全生命周期的安全管理体系，以防止原始敏感数据泄露与滥用。

10.2 核心安全目标

平台应实现以下核心安全目标：

a) 数据可用不可见：对个人敏感信息（身份证号、手机号等）进行去标识化处理，使外部机构接触到的均为无意义的随机编码；

b) 看得见信用：在有效保护身份信息的同时，应确保主体的经营能力、资产状况、历史信用等价值信息清晰呈现。

10.3 安全技术要求

平台应满足以下安全技术要求，包括但不限于：

c) 应通过网络安全等级保护三级测评；

d) 敏感数据应采用国密算法加密存储。

10.4 高可用要求

平台应采用高可用架构部署，建立数据备份与故障恢复机制，确保服务连续性和数据完整性。

10.5 数据匿名化

平台应支持数据匿名化处理。

注：匿名化处理应消除所有直接和间接标识符，以确保数据无法关联到个体。

10.6 安全审计

平台应建立安全审计机制。具体要求如下：

a) 对数据的每一次访问和使用应有授权、有记录、可溯源；

b) 审计日志应按法律法规要求留存，确保可追溯、可审计；

c) 应定期开展安全渗透测试和风险评估。

11 运行维护要求

11.1 运维组织

平台运营方应建立专门的运维团队，明确岗位职责和分工，并应制定运维管理制度和应急预案。

11.2 监控告警

平台应建立7×24小时监控体系。具体要求如下：

a) 应监控系统资源（CPU、内存、存储、网络）；
b) 应监控平台服务（API 响应时间、可用性、错误率）；
c) 应监控数据质量（完整性、准确性、更新时效）；
d) 应监控安全事件（异常访问、越权操作、数据泄露风险）；
e) 应设置分级告警阈值，并应实现告警自动通知和闭环处理。

11.3 接入管理

平台应建立接入管理制度。具体要求如下：

a) 应对数据提供方、数据使用方、数据服务方进行资质审核；
b) 应对接入连接器进行安全检测和认证；
c) 应对不合规或存在安全风险的接入方实行熔断或清退。

11.4 数据供应商管理

平台应建立数据供应商管理制度。具体要求如下：

a) 准入机制：数据提供方应通过资质审核和数据质量认证方可接入；
b) 评价机制：宜持续对数据供应商进行数据质量检测，检测维度包括数据质量、更新时效、合规性；
c) 禁用机制：宜对质量不合格数据供应商实行停用整改机制；
d) 退出机制：宜对质量持续不达标的供应商实行淘汰。

注：数据供应商可包括政务部门、征信机构、互联网平台、第三方数据服务商等类型。不同供应商的准入标准、评价周期和退出条件可根据数据类型和重要性分级管理。

11.5 变更管理

平台应建立变更管理流程。具体要求如下：

a) 所有变更应经过评审和审批；
b) 重大变更应制定回滚方案；
c) 变更操作应记录日志，保留变更历史。

11.6 应急响应

平台应建立应急响应机制。具体要求如下：

a) 应制定安全事件应急预案；
b) 应定期组织应急演练；
c) 应建立与监管部门的信息通报渠道。

参 考 文 献

[1] 国家数据局. 可信数据空间发展行动计划（2024—2028年）
[2] 国家发展改革委、国家数据局等. 国家数据基础设施建设指引.2024年12月
[3] 全国数据标准化技术委员会秘书处. 可信数据空间标准化研究报告（2025版）.2025年8月
[4] 全国人大常委会. 中华人民共和国数据安全法. 2021年
[5] 全国人大常委会. 中华人民共和国个人信息保护法. 2021年