ICS 35.240.68
CCS B 07

T/CS

团 体 标 准

T/CS XXX—2026

数字农业平台数据共享接口跨域接入规程

Code of practice for cross-domain access of data sharing interfaces on digital agriculture platforms

（征求意见稿）

2026 - XX - XX 发布　　2026 - XX - XX 实施

中国商品学会　　发 布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 接入架构 2
6 身份互认 3
7 接口封装 4
8 安全控制 5
9 审计追溯 6
10 运行管理 6

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专利的责任。

本文件由广东生态工程职业学院提出。

本文件由中国商品学会归口。

本文件起草单位：广东生态工程职业学院、宁夏回族自治区农业农村厅信息中心、杭州知止科技有限公司、山东政信大数据科技有限责任公司。

本文件主要起草人：李雪真、王聪、陈世杰、李俊青。

数字农业平台数据共享接口跨域接入规程

1 范围

本文件规定了数字农业平台数据共享接口跨域接入的接入架构、身份互认、接口封装、安全控制、审计追溯和运行管理要求。

本文件适用于分处不同信任管理域（如不同行政区域、不同运营主体）的数字农业平台之间，通过应用程序编程接口进行数据共享时的跨域接入设计、实施与运行管理。本文件不适用于涉及国家秘密的数据。

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 7408.1 日期和时间 信息交换表示法 第1部分：基本原则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37964 信息安全技术 个人信息去标识化指南

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

NY/T 3988 农业农村行业数据交换技术要求

NY/T 4063 农业信息系统接口要求

NY/T 4261 农业大数据安全管理指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据提供方平台 data provider platform

通过数据交换接口向其他平台提供数据资源的数字农业平台。

3.2

数据需求方平台 data requester platform

通过数据交换接口获取数据提供方平台数据资源的数字农业平台。

3.3

跨域接入 cross-domain access

数据需求方平台与数据提供方平台分别处于不同的信任管理域，通过接口调用方式获取数据提供方平台数据资源的交互过程。

3.4

数据交换接口 data exchange interface

跨域接入中，数据提供方平台向数据需求方平台暴露的、用于请求和返回约定数据集的 API 端点及其调用规则。

3.5

跨域接入网关 cross-domain access gateway

数据提供方平台部署的、作为数据交换接口唯一对外暴露点，对跨域接入实施转发、鉴权、限流和审计的装置或软件。

3.6

域间信任凭证 inter-domain trust credential

由数据需求方平台所属信任管理域的身份服务签发、经数据提供方平台所属信任管理域验证并接受的数字凭证，用于在跨域接入中标识调用方身份和授权范围。

3.7

接入审计记录 access audit record

跨域接入过程中，对每一次数据交换接口的调用请求、响应结果和关键上下文信息进行结构化记录所形成的日志条目。

4 缩略语

下列缩略语适用于本文件。

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

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

IP：互联网协议（Internet Protocol）

JWT：JSON Web 令牌（JSON Web Token）

TLS：传输层安全协议（Transport Layer Security）

5 接入架构

5.1 总体结构

跨域接入应采用由跨域接入网关、域间信任凭证和数据交换接口构成的三层结构。数据提供方平台应部署跨域接入网关，作为数据交换接口的唯一对外暴露点，数据交换接口不应直接对外提供访问；数据需求方平台应通过本域身份服务获取域间信任凭证；双方平台之间的全部数据交换接口调用应经由跨域接入网关转发和鉴权。跨域接入网关的部署和配置应符合 GB/T 22239 中对相应等级保护对象的安全区域边界和安全计算环境要求。

5.2 角色与职责

5.2.1 数据提供方平台应履行以下职责：

a) 维护数据交换接口目录，向数据需求方平台提供接口标识、名称、版本号、数据项清单和调用频次上限和单次返回数据量上限；

b) 验证域间信任凭证的有效性和授权范围；

c) 记录接入审计记录，并保证记录的完整性；

d) 维护跨域接入授权清单，并至少每年复核一次；

e) 监测数据交换接口的可用性，并按 10.1 的规定通知计划内停机。

5.2.2 数据需求方平台应履行以下职责：

a) 向本域身份服务申请域间信任凭证，并在调用数据交换接口时附带该凭证；
b) 按照数据提供方平台公布的接口版本和参数规范发起调用；
c) 对本平台发起的跨域接入行为承担身份溯源责任；
d) 按声明的业务目的使用所获取的数据，在约定期限内留存或删除，并承担相应的数据安全保护责任。

5.3 接入前置条件

数据提供方平台在开放数据交换接口之前，应完成以下检查并留存记录：

a) 接口所涉数据已按照 NY/T 4261 完成安全分类分级，且共享范围与分类分级结论一致；
b) 接口调用频次上限和单次返回数据量上限已明确并写入接口目录；
c) 跨域接入网关已完成与数据提供方平台现有身份服务的对接联调，并留存联调记录；
d) 接口所涉数据涉及个人信息的，已确认数据提供方平台按 GB/T 35273 完成个人信息保护影响评估，并在接口目录中标注该接口的个人信息字段清单；
e) 跨域接入网关及其所承载的数据交换接口已确定安全保护等级，并已按 GB/T 22239 相应等级的要求完成安全保护措施配置。

5.4 接入流程

5.4.1 跨域接入应按以下流程实施：

a) 数据需求方平台按第 6 章的规定获取域间信任凭证；
b) 数据需求方平台按第 7 章的规定封装请求，并经跨域接入网关发起调用；
c) 跨域接入网关按 6.2 的规定验证域间信任凭证，按 8.2 的规定执行授权判定，按 8.3 的规定执行调用频次控制；
d) 验证和授权通过后，数据提供方平台按 7.3 的规定返回响应，并按 8.1 的规定实施传输安全和敏感数据处理；
e) 跨域接入网关按第 9 章的规定生成并保存接入审计记录。

5.4.2 跨域接入的交换方式、交换流程及质量控制应符合 NY/T 3988 的规定；数据交换环节的身份鉴别、访问控制、安全传输、操作抗抵赖、过程可追溯和接口安全等要求，应符合 GB/T 39477 中关于共享数据交换阶段的相应规定。

6 身份互认

6.1 域间信任凭证的获取

6.1.1 数据需求方平台应通过授权码授权模式（authorization code grant）向本域身份服务申请域间信任凭证，不应采用隐式授权模式（implicit grant）。

6.1.2 授权码的有效期不应超过 10 min。授权码应一次性使用，未被使用的授权码应在有效期届满后失效。

6.1.3 域间信任凭证应采用 JWT 格式，并在载荷中包含以下声明：签发者标识（iss）、主体标识（sub，即数据需求方平台标识）、受众标识（aud，即数据提供方平台标识）、签发时间（iat）、过期时间（exp）、凭证唯一标识（jti）和授权范围（scope）。域间信任凭证应采用非对称密钥算法签名，签发者应向数据提供方平台提供用于验证签名的公钥；凭证载荷中不应包含个人信息等敏感数据。

6.2 域间信任凭证的验证

6.2.1 数据提供方平台的跨域接入网关应对域间信任凭证执行以下验证，任一验证不通过应拒绝接入：

a) 签名验证：使用签发者公布的公钥或共享密钥验证 JWT 签名；网关应预先配置允许的签名算法清单，仅接受清单内的算法，不应接受“none”算法，也不应依据凭证头部声明的算法选择验证方式；

b) 受众验证：aud 声明值应与本平台标识一致；

c) 时效验证：当前时间不应晚于 exp 声明值指明的时刻，且 iat 声明值不应晚于当前时间 5 min 以上；跨域双方应约定允许的时钟偏差，偏差不应大于 5 min；

d) 主体授权验证：sub 所标识的数据需求方平台应在数据提供方平台的跨域接入授权清单中（授权判定的具体要求见 8.2）。

6.2.2 域间信任凭证即跨域接入中使用的访问令牌，其生命周期不应超过 1 h。确需延长持续访问时间的，应通过刷新令牌机制获取新的访问令牌；刷新令牌的有效期不应超过 24 h，并应采用轮换机制，每次刷新后原刷新令牌失效，不应直接延长单个令牌的有效期。

6.3 凭证撤销与重放防护

6.3.1 数据需求方平台发现域间信任凭证泄露或所属平台身份状态变更时，应在 30 min 内向本域身份服务发起凭证撤销，并将撤销事件通知数据提供方平台。数据提供方平台应在收到撤销通知后，将已撤销凭证的唯一标识（jti）加入拒绝列表，更新时延不应超过 30 min。

6.3.2 跨域接入网关应维护已使用 JWT 的唯一标识（jti）短期缓存，缓存保留时间不应短于对应令牌的剩余有效期与约定时钟偏差之和。同一 jti 的凭证在有效期内重复提交时，应拒绝接入并生成告警审计记录。

7 接口封装

7.1 接口描述

7.1.1 每一个数据交换接口应在接口目录中提供以下描述项：接口标识、接口名称、版本号、请求方法（GET 或 POST）、请求地址、请求参数列表、响应数据项列表、单次最大返回记录数、调用频次上限、分页参数上限、接口所涉数据的安全级别、个人信息字段清单（接口涉及个人信息时）和错误码列表。接口描述项的结构应与 NY/T 4063 中接口描述的要求保持一致。

7.1.2 接口版本号应采用“主版本号.次版本号”格式，初始版本号应为 1.0。当数据项删除、数据项语义变更或请求参数必填性变更时，应提升主版本号；仅新增可选数据项或新增可选请求参数时，可提升次版本号。

7.2 请求封装

7.2.1 数据需求方平台发起数据交换接口调用时，应在 HTTPS 请求头中携带“Authorization: Bearer <域间信任凭证>”。

7.2.2 请求参数应采用 JSON 格式（“Content-Type: application/json”）或查询字符串格式传递。采用 JSON 格式时，请求体中应包含 requestId 字段；采用查询字符串格式时，应在查询字符串中包含 requestId 字段。requestId 的值为本次调用的全局唯一标识，用于审计关联。

7.2.3 请求的 TLS 版本不应低于 TLS 1.2。涉及 NY/T 4261 中重要数据、核心数据的接口，跨域接入网关应支持 TLS 1.3 及以上版本的协商能力，实际启用的 TLS 版本不应低于 TLS 1.3。

7.3 响应封装

7.3.1 响应体应包含以下顶层字段：requestId（与请求一致）、status（取值为 success 或 fail）、data（成功时返回数据集，失败时为空）、message（失败时的错误描述）、errorCode（失败时的错误码，取值应与接口目录中声明的错误码列表一致）和 timestamp（响应生成时间，应采用 GB/T 7408.1 规定的日期时间表示法）。
7.3.2 请求参数中应包含分页参数 page 和 pageSize。对于超过单次最大返回记录数的查询请求，响应中应包含 page 和 pageSize 字段，并应在接口目录中声明分页参数上限。

7.4 错误处理

7.4.1 数据提供方平台应对每一类可预期的调用失败返回明确的 HTTP 状态码和响应体 status: fail，不应以 HTTP 200 状态码掩盖业务失败。
7.4.2 因凭证无效、授权不足或请求格式错误导致的失败，不应返回 data 字段中的任何数据片段。
7.4.3 可预期的调用失败应按以下规则返回 HTTP 状态码：请求参数或请求格式错误返回 400；凭证无效或已过期返回 401；授权范围不足返回 403；接口标识或接口版本不受支持返回 404；调用频次超限返回 429；数据提供方平台内部处理失败返回 500。
7.4.4 错误描述信息不应包含数据提供方平台的内部实现细节，也不应泄露接口目录之外的数据项名称。

8 安全控制

8.1 传输安全

8.1.1 跨域接入的全部数据交换接口调用应使用 HTTPS，不应使用明文 HTTP。
8.1.2 涉及 NY/T 4261 中重要数据、核心数据的接口，应在 TLS 通道之上对响应数据中的敏感字段实施应用层加密或脱敏处理。应用层加密应采用国家密码管理部门认可的密码算法。脱敏处理应符合 GB/T 37964 的方法要求。

8.2 访问控制

8.2.1 跨域接入网关应依据域间信任凭证中的授权范围声明（scope 或等效声明）对每一次数据交换接口调用执行授权判定。授权范围应至少区分“只读查询”和“批量导出”两类操作权限，并应在 scope 声明中分别以 read 和 export 标识。
8.2.2 授权判定应采用默认拒绝策略：未在授权清单中明确允许的数据交换接口和数据项，跨域接入网关应拒绝访问。授权清单及其变更应由数据提供方平台留存记录。
8.2.3 涉及个人信息的接口，数据需求方平台应在调用前确认数据提供方平台已按照 GB/T 35273 完成个人信息保护影响评估，并在接口目录中标注该接口的个人信息字段清单。数据需求方平台应留存确认记录。

8.3 调用频次与容量控制

8.3.1 数据提供方平台应在跨域接入网关上对每一个数据需求方平台设置数据交换接口调用频次上限。频次上限应按接口分别设置，并结合接口所涉数据的安全级别和数据需求方平台的业务需要确定。
8.3.2 当同一数据需求方平台在 1 min（滑动窗口）内超出频次上限时，跨域接入网关应返回 HTTP 429 状态码，并应返回重试等待时间（Retry-After），同时记录限流审计事件。
8.3.3 跨域接入网关应支持按接口、按数据需求方平台分别设置调用频次上限，并应具备在超限调用或异常调用情况下的限流和告警能力。

8.4 数据最小化

8.4.1 数据需求方平台应在请求中仅声明完成本次业务目的所必需的数据项。跨域接入网关应拒绝请求参数中要求返回接口目录未列明数据项的调用。数据需求方平台不应超出申请时的业务目的使用和对外提供所获取的数据；批量导出应经数据需求方平台内部授权，并留存授权记录。
8.4.2 数据需求方平台应在业务目的完成后，按与数据提供方平台约定的期限删除或匿名化所获取的数据，并留存处理记录。

9 审计追溯

9.1 审计记录内容

9.1.1 跨域接入网关应对每一次数据交换接口调用生成接入审计记录，记录至少包含以下字段：

a) requestId；
b) 调用时间戳（精确到秒，采用 GB/T 7408.1 规定的格式）；
c) 数据需求方平台标识（取自域间信任凭证 sub）；
d) 数据提供方平台标识；
e) 数据交换接口标识及版本号；
f) 请求操作类型（查询/导出/其他）；
g) 响应状态（success/fail）及错误码；
h) 返回记录数；
i) 源 IP 地址；
j) 域间信任凭证的唯一标识（jti）；
k) 授权范围（scope）。

9.1.2 对于因凭证验证失败、授权拒绝或限流拦截而未实际进入数据返回流程的接入尝试，仍应生成接入审计记录。

9.2 审计记录的留存

9.2.1 接入审计记录的在线留存期限不应少于 6 个月。
9.2.2 涉及 NY/T 4261 中重要数据、核心数据的接口，其接入审计记录的在线留存期限不应少于 12 个月。

9.3 审计记录的完整性与可追溯性

9.3.1 接入审计记录应写入防篡改存储，或采用密码学手段保证记录自生成后不可抵赖地可验证其未被修改。记录存储系统应对审计记录的写入操作实施独立于跨域接入网关的访问控制。跨域接入网关与审计记录存储系统应采用一致或同步的时间源，两者之间的时间偏差不应大于 1 s。
9.3.2 数据需求方平台和数据提供方平台应能够以 requestId 为关联键，在双方审计记录中定位同一次跨域接入行为。任何一方因审计追溯需要调取对方记录的，对方应在收到请求后 5 个工作日内提供。调取的记录应以加密方式传输，双方应留存调取和提供记录。
9.3.3 跨域接入网关应每月生成审计摘要报告，至少包含：调用总次数、成功/失败比、按数据需求方平台分组的调用量、限流拦截次数和凭证验证失败次数。摘要报告应提交至双方平台的安全管理责任人。摘要报告应于次月前 10 个工作日内提交，并至少留存 12 个月。

10 运行管理

10.1 接口可用性与停机管理

10.1.1 数据提供方平台应持续监测跨域接入所涉及数据交换接口的可用性。接口月度可用性不应低于99.5%。接口月度可用性按式（1）计算：

$$A=\left(1-N_{\mathrm{f}}/N\right)\times 100\% \quad \cdots\cdots (1)$$

式中：

A——接口月度可用性，以百分数表示；

N_f——统计周期内因数据提供方平台原因导致失败的接口调用次数，单位为次；

N——统计周期内数据需求方平台针对同一接口发起的调用总次数，单位为次。

10.1.2 因数据需求方平台自身原因（如凭证无效或已过期、授权不足、请求参数错误、超出调用频次上限）导致的失败调用，以及数据提供方平台按本条规定通知的计划内停机期间的调用，不计入N_f；统计周期内无调用时，不按式（1）计算接口月度可用性。

10.1.3 数据提供方平台应至少提前5个工作日向数据需求方平台通知计划内停机的安排。

10.2 接口目录与版本变更管理

数据提供方平台应在数据交换接口新增、下线、版本升级或参数规范变更时同步更新接口目录，并至少提前15个工作日通知数据需求方平台；接口下线的通知期不应少于30个工作日。数据需求方平台应在收到通知后按新的接口目录调整调用实现。

10.3 定期检查与改进

双方平台应每年至少组织一次跨域接入的联合检查，检查内容包括接口目录与授权清单的一致性、域间信任凭证的签发与失效管理、接入审计记录的完整性以及安全控制措施的有效性。检查发现的问题应明确整改责任方和整改期限，并留存整改记录。