|  |  |
| --- | --- |
| ICS |  |
| CCS | |  | | --- | |  | |

技术标准

XXXX—XXXX

农业投入品经营流通与溯源回收监管一体化系统技术规范（总）

Technical specification for integrated system of agricultural input management circulation and traceability recovery supervision

XXXX - XX - XX发布

XXXX - XX - XX实施

       发布

目次

[前言 II](#_Toc24911)

[1 范围 3](#_Toc13039)

[2 规范性引用文件 3](#_Toc25628)

[3 术语和定义 3](#_Toc32476)

[4 总体要求 5](#_Toc628)

[5 功能要求 5](#_Toc8212)

[6 技术要求 9](#_Toc8748)

[7 管理要求 11](#_Toc20071)

[8 安全要求 12](#_Toc10209)

[9 运行维护要求 13](#_Toc24548)

1. 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XXXXX会提出并归口。

本文件起草单位：河北农业大学；北京艾格地赞农业科技有限公司；北京威斯得农业科技有限公司。

本文件主要起草人：张爱军，张鑫，杨晓楠，李文超，付鑫，弓运泽、王梅，李魏铭，刘冬梅，张爱民，谷立涛等。

农业投入品经营流通与溯源回收监管一体化系统技术规范（总）

* 1. 范围

本文件规定了农业投入品经营流通与溯源回收监管一体化系统的术语和定义、总体要求、功能要求、技术要求、管理要求、安全要求、运行维护要求。

本文件适用于农业投入品经营流通与溯源回收监管一体化系统。

* 1. 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 4205 人机界面标志标识的基本和安全规则　操作规则

GB/T 17004 防伪技术术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28827.1 信息技术服务运行维护 第1部分 通用要求

GB/T 28827.2 信息技术服务 运行维护 第2部分：交付规范

GB/T 28452 信息安全技术 应用软件系统通用安全技术要求

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 33745 物联网 术语

GB/T 38155 重要产品追溯 追溯术语

GB/T 38157 重要产品追溯-追溯管理平台建设规范

GB/T 38158 重要产品追溯 产品追溯系统基本要求

GM/T 0054 信息系统密码应用基本要求

* 1. 术语和定义

GB/T 17004、GB/T 31167、GB/T 33745、GB/T 38155界定的以及下列术语和定义适用于本文件。

农业投入品 agricultural input

在农产品生产过程中使用或添加的农用生产资料产品，包括种子、种苗、肥料、农药、兽药、饲料及饲料添加剂、农膜等。

系统system

基于追溯码、文件记录、相关软硬件设备和通信网络，实现现代信息化管理并可获取产品追溯过程中相关数据的集成。

[GB/T 38155，定义2.67有修改]

参与方 participant

在供应链中从事产品初级生产、生产加工、包装、仓储、运输、配送、销售、消费(使用)等相关业务的组织或个人。

[GB/T 38155，定义2.5有修改]

追溯单元 traceability unit

需要对其历史、应用情况或所处位置的相关信息进行记录、标识并可追溯的单个产品、同一批次产品或同一品类产品。

[GB/T 38155，定义2.47]

基本追溯信息basic traceability information

能够实现追溯系统中各参与方之间有效链接的必需信息。

[GB/T 38155，定义3.1]

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟资源池，并可按需自助获取与管理资源的模式注:资源实例包括服务器、操作系统、网络、软件、应用与存储设备等。

[GB/T 31167，定义3.1]

物联网 internet of things

通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。

[GB/T 33745，定义 2.1.1]

区块链 blockchain

在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的区块链式数据结构，实现和管理事务处理的模式。

防伪技术 anti-counterfeiting techniques

为了达到防伪目的而采取的，在一定范围内能准确鉴别真伪并不易被仿制和复制的技术。

[GB/T 17004，定义2.2]

* 1. 总体要求

4.1 系统的建设、运行应符合国家相应法律法规与标准的规定，并充分满足管理部门、消费者、供应链企业等不同类型用户的差异化需求。

4.2 系统建设方应明确其在供应链中的位置，并将涉及的供应链环节中质量安全相关信息作为重要内容，以便在供应链上形成全程信息链条。

4.3 参与方应建立数据存储和管理机制，可利用区块链、防伪等技术完整记录追溯信息，确保数据真实、准确、完整。

4.4 系统应能实现内部追溯和外部追溯，对接追溯主体的内部管理信息系统和追溯参与方的供应链信息系统。

4.5 系统应对追溯信息进行分用户管理，向消费者、相关部门、相关企业等用户按需要、按权限提供追溯信息。

4.6 系统宜使用云计算、物联网、区块链、防伪技术等信息技术建设。

* 1. 功能要求

认证管理

应对用户基本信息、土地信息及作物种植信息的实名认证与统一管理。主要是区块链中节点根据自身的需求输入相关的信息在系统中进行身份的注册，管理员审核通过后，输入相关的信息便可登录系统进行相关的操作。可以避免一些没有授权的恶意节点加入供应链系统中。能更好地保护数据安全性以及数据的可追溯性， 也较为全面地考虑到消费者溯源的途径以及参与度。

生产供应监督管理

在监管部门认证授权后，将农业投入品的原始生产信息与供应出售信息上传至联盟链。监管部门作为系统中最重要的身份之一，主要作用是审查农业投入品生产过程中的质量安全信息。与此同时，监管节点可以查看产业链上其他节点的操作信息。当发生了农业投入品质量问题时，监管部门需要对问题产品进行追踪和召回，同时对涉及的相关企业作相应的惩罚措施。

经营流通管理

监测农业投入品的经营流通过程，记录经销商、零售商及物流的全流程的购销流通信息，并以零售商作为最小的单位节点，建立销售地域网络，通过购销流通趋势预测实现供应调度优化。

5.3.1 购销流通记录/**供应链交易追溯记录**

在农业投入品完成上游供应链各环节流转至零售终端后，运营主体首先通过调用相关/智能合约对商品属性及合规性进行验证。验证通过后，零售终端/商业实体需向监管平台提交包括商户主体资质信息、经营许可证照、库存管理数据等结构化业务信息。系统集成平台系统基于物联网设备采集的物流数据、区块链存证的交易凭证以及第三方质检报告，自动生成涵盖生产、流通、零售全链条的数字化追溯记录。该分布式账本信息通过经销商和终端零售商的业务系统接口认证后，通过加密传输协议逐级上报至联盟链分布式账本网络，形成不可篡改的农产品供应链溯源闭环。

5.3.2 销售地域网络

以零售商作为最小的单位节点，以零售商所在城镇作为单位销售区域，建立销售地域网络，形成销售网络拓扑结构，并结合GIS技术建立可视化的销售地域网络模型。

5.3.3 作物病害分析

基于单位销售区域内的土地信息与作物种植信息，统计该单位销售区域内存在的作物类型与种植面积，并分析不同作物类型对应的病害预测信息与投入品需求信息。

5.3.4 趋势分析预测

基于历史购销数据，分析单位销售区域内农业投入品的购销流通趋势，并预测未来销售周期的预测购销数据。

5.3.5 市场响应调度

依据销售地域网络内各个单位销售区域的预测购销数据，制定市场响应策略，调整农业投入品的供应计划，并通过销售地域网络模型展示农业投入品的市场余量分布。

信息溯源存储

搭建基于联盟链的读取写入网络及链上数据库，记录并存储农业投入品在全生命周期内的溯源信息。

5.4.1 联盟链网络

联盟链网络由多级应用链架构构成，包含生产商节点、监管主体节点、分销商节点、零售商节点、生产溯源节点（农户）及逆向物流节点（回收网点）组成的异构区块链网络，通过交互协议栈实现跨链互操作。系统构建基于四层核心模块：

（1）链域治理模块

实现异构链群组动态扩展功能，采用基于角色的访问控制（RBAC，Role-Based Access Control）模型管理生产商链、监管链、分销链、零售链及农业溯源链的节点准入权证，支持智能合约驱动的链级权限矩阵更新。

（2）链适配中间件

部署模块化插件动态加载机制，通过跨链互操作协议转换器实现企业联盟链与跨链路由的协议级对接，内置EVM/WASM双模执行引擎处理链间服务调用请求，集成面向链上预言机的数据溯源服务网关。

（3）授权日志存证系统

构建基于零知识证明的可验证访问控制账本（VACL，Virtual Access Control List），采用Merkle-Patricia树结构固化跨链身份认证全生命周期记录，实现审计不可抵赖性，通过IPFS实现认证元数据链外存储与链上摘要锚定。

1. 互操作路由枢纽

部署PolyMesh中继架构，采用状态通道监控机制侦听跨链事务请求队列，基于门限签名方案（TSS，Threshold Signature Scheme）实现跨链原子交换，通过去中心化标识符（DID，Decentralized Identifier）解析目标链资源地址，构建包含BFT共识的跨链事务协调器完成跨链状态验证与事务确认回执（PoC）同步。

5.4.2 链上数据存储

通过在应用链区块头（Block Header）内嵌Merkle Root摘要值，并在区块体（Block Body）构建Merkle Patricia Trie与关系型数据库的混合存储结构，形成基于区块链状态机的持久化数据层。采用零知识证明算法对农业投入品流转全量信息进行同态加密处理，将单次供应链事件封装为原子化交易单元，经SHA-3哈希运算后锚定至默克尔树的叶子节点。系统需研发加密溯源审计树数据结构，并通过RLP编码将其完整表征体系固化至关系数据库，并在交易元数据中植入带时间戳的数据库索引指针，实现可验证数据存证与具有时序特征的凭证链追溯机制。

5.4.3 购销信息溯源

初始应用链发送溯源请求，且目标应用链验证通过后，在初始应用链与目标应用链之间建立私有数据通道，通过私有数据通道实现不同应用链之间的信息交互，并依据链上数据库中的溯源有序树的节点，查询农业投入品全生命周期内的溯源信息。消费者也可通过应用平台的接口进行溯源信息查询，系统在后台查询到此产品所有涉及到交易合约地址，通过合约地址获取到供应链上的交易的哈希值，最后通过哈希值查询到真实的溯源数据，完成溯源。

配方定制推荐

基于农户登记的土地信息、作物种植信息以及现有病害现象，在零售过程中向农户推荐农业投入品的最佳定制配方。

废品回收管控

搭建农业投入品废弃物的回收管控网络，并引入回收激励机制，评估各类型农业投入品与不同销售区域的回收价值。

5.6.1 网点服务

配置农业投入品废弃物回收网点，并向农户提供农业投入品废弃物的回收网点信息，其中，回收网点信息包括网点地理位置、联系方式、服务时间、服务内容及废弃物信息。

5.6.2 分类评估

基于农业投入品废弃物的危害程度与再利用潜在价值，对不同类型的农业投入品废弃物进行分类评估。建立回收激励机制，基于农业投入品的分类结果与回收成分，评估回收网点及农户个人的回收参与率及积分奖励。

基于农业投入品废弃物的评分体系，为不同等级的废弃物设定不同的回收积分，并匹配该废弃物对应的农业投入品类型，获取所在销售区域在当前消费周期内对该农业投入品类型的历史出售数据与回收数量，再计算每种农业投入品类型的单周期回收率，通过网点积分公式计算回收网点在当前销售周期的积分。

5.6.3 网络集成

集成销售地域网络，通过可视化模型实现数据交互与信息共享，展示不同销售区域的废弃物回收能力。

5.6.4 报告分析

生成定期的分析报告，评估回收效果。

实时汇总展示

提供经营流通与回收信息的可视化展示。

* 1. 技术要求

用户角色

满足多用户角色同时使用标准，实现监管端用户、农资经营端用户、农户一体化系统，数据实时互通的标准。用户系统中将各用户分成组，又特别指定出具有特殊权力的超级用户。系统管理员在多用户系统中增加新用户时，他要指定出用户名，口令、组别，对系统内各文件资源的使用范围，进入系统后自动进入的自录和调用的程序，限定了用户对系统的使用权限。只有在系统管理员完成上述工作后，操作人员才有可能按照上述限定进行登录操作，作为这个新建的用户进入多用户系统工作。

系统架构

采用前后端分离架构的系统，其技术方案设计应遵循高可维护性与可扩展性框架标准。

（1）并行开发机制：解耦式架构支持客户端与服务端研发团队的同步工程实施，通过标准化接口契约解除前后端开发的时序依赖关系，实现敏捷开发周期管理。

（2）异构技术选型能力：允许面向表现层（front-end）与业务逻辑层（back-end）采用差异化的技术路线。前驱端可根据交互需求自主选型现代化框架体系（React/Vue/WebAssembly），后驱端可适配Spring Boot/Django等不同服务架构，形成最优化的全栈技术解决方案。

（3）弹性扩展架构：具备横向扩展能力独立部署的特性，支持通过负载均衡机制灵活拓展展示层CDN节点或业务层微服务实例，实现系统吞吐量与并发处理能力的线性提升。

（4）动态交互优化：基于Ajax/Fetch异步通信技术实现局部DOM更新机制，配合Service Worker离线缓存策略与资源预加载技术，显著降低首屏加载时延（FP/FCP）并优化交互响应延迟(INPUT Latency)，保障关键用户体验指标(Web Vitals)达标。

（5）契约驱动协作模式：通过OpenAPI/Swagger规范建立RESTful接口定义语言（IDL），形成具备版本控制能力的服务合约，实现跨团队高效协作的DevOps集成环境。

（6）低耦合维护体系：依据单一职责原则（SRP）划分服务边界，通过接口隔离实现变更影响域的精确控制，有效降低模块间的耦合度（Coupling Coefficient），提升系统的可迭代性与故障隔离能力。

开发语言

（1）以Java作为首要开发语言，应符合多终端、跨平台、跨系统的应用程序工业级标准。基于OOP理论体系，Java强制执行代码单元必须在类边界内定义（除基本数据类型外）。通过抽象、接口契约与多态调度构成的模块化工程范式，为系统提供可验证的代码正交性及架构演进能力。

（2）平台抽象层架构：依托JVM规范定义的标准指令集（JVM bytecode），Java编译器将源代码转换为与硬件架构解耦的中间表示形式（IR），按照配合各系统完整实现WORA（Write Once， Run Anywhere）原则，确保编译产物在x86/ARM架构及主流操作系统间的ABI兼容性。

（3）托管堆内存系统：采用分代假设指导的自动内存管理子系统（含Young/Old代划分），通过复合垃圾回收算法（如Mark-Sweep-Compact）与并发标记技术（CMS/G1），实现无需开发者干预的内存生命周期管控。

（4）编译时类型完整性验证：作为静态类型系统，Java通过类型推理算法（在编译前端阶段）对变量声明、方法签名及泛型参数执行约束检查（包含协变/逆变验证），构建编译期类型安全保障，消除隐式转换与空指针解引用等经典运行时缺陷。

后端框架

首选Spring Boot框架构建体系架构，集成MyBatis-Plus增强型ORM组件实现数据持久化，配置Druid工业级数据库连接池保障资源管理，结合Redis分布式缓存组件进行热点数据预存取。符合复杂业务系统的高可用性要求，满足高并发、大数据量场景下的弹性伸缩需求，具备ORACLE TPC-C基准测试级别的性能承载能力，适配千万级用户规模的分布式系统部署需求。

管理后台前端框架

首选Vue，满足灵活配置、易于修改的标准。Vue使用简洁的模板语法，可以直接将数据和DOM元素绑定在一起，而不需要手动操作DOM。这样可以提高开发效率，也便于维护和测试。Vue利用了JavaScript的对象属性特性，实现了数据和视图之间的双向绑定。当数据发生变化时，视图会自动更新，反之亦然。这样可以避免频繁的DOM操作，提高性能和用户体验。Vue不是一个完整的框架，而是一个核心库，它只关注视图层。这样可以让开发者根据自己的需求，灵活地选择其他的库或工具来搭配使用，如路由器、状态管理器、UI库等。Vue也提供了一些官方的打展库，如Vuex、Vue Router、Vue CLI等，来方便开发者构建大型的单页应用。Vue有着简单易学的API和文档，以及丰富的社区资源和教程。Vue也有着良好的兼容性，可以运行在各种浏览器和设备上。Vue还有着优秀的开发者工具，如浏览器插件、调试器、脚手架等，可以帮助开发者快速地搭建和调试应用。

小程序框架

首选原生技术，满足稳定性、安全性的标准。原生框架由官方开发，具有官方支持，能够及时得到修复和更新。原生框架易于上手，学习成本低。原生框架采用原生组件，运行速度较快，用户体验好。

应用部署

首选Nginx(负载均衡) + Tomcat ，满足可负载均衡、灵活调配软硬件环境的标准。它的优点是基于特定环境、配置简单、使用灵活、成本低廉，可以满足大部分的负载均衡需求。

数据库

首选Mysql 5.7.x，满足低成本、高可用、数据安全程度高的标准。能够使用现有的操作系统环境来提供跨平台的性能优化和访问控制。该解决方案的优势在于它可以保证数据库的安全性、表现力和实用性。基于SQL的NoSQL和存储引擎技术，能够提供高性能、低延迟和可扩展性，可以支持Relational、NoSQL和时序数据库，有利于分布式数据库的设计，从而提供良好的高可扩展性。可以使用新一代存储引擎技术和实时数据库计算，加快数据库的查询速度和更新速度。此外，还内置了密码保护技术，可以保护数据库的安全性并提供完整的审计支持。它还提供了一系列最新的优化特征，具有更好的缓存管理和查询管理功能，可以更有效地管理各种存储引擎上的数据，从而保证数据库表现力、安全性和实用性。

系统安全与稳定

满足高可用、大并发、数据通信传输协议加密的标准。首先，数据传输加密保护了数据的机密性。通过使用加密算法，将原始数据转化为一种无法直接识别的密文，即使泄露也无法被解读。这样可以防止黑客入侵或者监听者获取数据的敏感信息，保护了用户和组织的隐私。其次，数据传输加密保证了数据的完整性。在数据传输过程中，通过加密算法，可以为数据生成一种数字签名或者校验和，用于验证数据在传输过程中是否被篡改。一旦检测到数据的完整性有问题，就可以及时采取措施阻止对数据的非法篡改。最后，数据传输加密保障了数据的可用性。泄露数据不仅会导致信息安全问题，还可能瘫痪整个系统。数据加密可以防止黑客获取敏感数据造成的恶意破坏，保证了数据的正常运转。

* 1. 管理要求

配置管理要求

配置管理应包括以下几方面要求：

（1）具有通过配置，实现多终端查询溯源数据。

（2）具有对溯源的业务流程和业务信息进行灵活配置和修改的能力。

多业务类型支持要求

系统应支持不同业务类型的场景，对不同业务实现便捷地适配。

身份标识要求

溯源应用可对系统中的产品或溯源平台调用者身份信息进行固证。

产品目录管理

应根据需要调整溯源总体分类目录，确定纳入溯源体系的产品类别及下级分类目录。

产品登记管理

应支持通过平台登记产品信息，包括但不限于溯源产品信息登记、修改、审核等功能。支持对产品信息变更权限的管理。

问询、投诉管理

应包括以下方面：

（1)建立信息响应和反馈机制。

（2）能受理溯源方面的问询和投诉。

* 1. 安全要求

网络安全要求

应保证系统中各节点数据网络传输过程的安全性，防止网络劫持和数据窃听等。

操作审计要求

应保存调用者对系统数据进行全生命周期操作过程中的审计数据，以便事后查阅分析。

数据隐私性要求

应满足数据隐私性要求，提供隐私保护方案保护参与方隐私数据。系统中数据存储在公共的账本中，数据公开，但是在实际项目中，并非所有的数据都要公开被验证，相关的隐私数据涉及企业的运营，如果隐私信息被篡改、伪造，造成溯源信息与真实数据不匹配，会影响企业和监管部门的信誉度。

数据安全要求

数据安全管理应满足以下要求：

1. 溯源系统的数据安全管理标识应符合 GB/T 4205 的要求。
2. 溯源系统的数据安全性要求应符合 GB/T 38157 的要求，网络安全等级应符合GB/T 22239的要求，应用软件的安全等级应符合 GB/T 28452 的要求。
3. 应采取容错性设计，匹配网络安全防范措施。
4. 密码应用及密码安全保护措施应符合 GM/T 0054 的要求。
5. 应具备追溯信息防篡改、防攻击、访问权限控制等安全防护能力。
6. 应具有完整的用户操作日志记录功能，且不可随意更改。
   1. 运行维护要求

应具备完善的运维管理体系并严格按照体系执行：

（1）系统运行维护基本要求应符合 GB/T 28827.1的要求：考虑环境的内外部因素，在治理要求的指导下，根据服务场景，识别服务能力需求，围绕人员、过程、技术、资源能力四要素，策划、实施、检查和改进运行维护能力体系，向各种服务场景赋能，通过服务提供，实现服务价值。针对能力建设、人员、过程、技术、资源建立关键指标。定期评价运行维护服务能力成熟度，衡量能力水平差距，以持续提升运行维护服务能力。

（2）系统运行维护的交付应符合 GB/T 28827.2 的要求。依据服务目录与需方确认服务级别协议；确保服务级别协议内容完整准确；编制交付实施计划、交付检查计划和交付改进计划；配备符合能力要求的管理人员和专业人员；明确职责分工、服务流程和关键技术要求，必要时提供服务手册和技术手册；准备必要的资源，如备件、工具、服务平台和知识库；明确考核要求、计算办法和奖惩措施；明确服务交付过程中的安全要求，并采取保障措施，如签署保密协议等；明确服务交付过程中可能存在的各种风险，制定风险规避计划；与需方就必要信息达成共识，如时间计划、人员配备、投诉受理渠道及流程等；明确供需双方产生异议的处理原则；明确供需双方在交付过程中产生遗留问题的处理原则。