ICS 35.020
CCS L60

T/ZGCMCA

中 国 移 动 通 信 联 合 会 团 体 标 准

T/ZGCMCA 022—2024

危险化学品数字身份认证通用规范

General specifications for the digital identity authentication of dangerous chemicals

2026－02－07 发布　　2026－02－07 实施

中国移动通信联合会　　发 布

目　　次

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。

本文件由中国移动通信联合会提出并归口。

本文件起草单位：四川易链科技有限公司、电子科技大学、赛飞特工程技术集团有限公司、成都成电邦粹科技有限公司、上海网博网络科技有限公司、深圳英智源智能系统有限公司、成都成飞航空产业发展有限责任公司、广州为乐信息科技有限公司、上海飞域实验室设备有限公司、河北科技师范学院、上海润吧信息技术有限公司、密尔克卫智能供应链服务集团股份有限公司、重庆大学、眉山市应急救援指挥中心（眉山市减灾中心）、眉山职业技术学院(眉山技师学院)、四川省人工智能行业协会、眉山市大数据产业发展有限公司、四川省盈达锂电新材料有限公司、盐亭盈基生物质能源开发有限公司、四川启明星铝业有限责任公司、东莞市广和精细化工有限公司、四川兴荣科科技有限公司、深圳市成为信息股份有限公司、四川中科兴业高新材料有限公司、四川欣乾环境技术有限公司、智菲科技集团有限公司、公诚管理咨询有限公司、中标政联咨询（北京）有限公司。

本文件主要起草人：沈长军、桂勋、孟强、孙超、张彬、谭轼、谢绍国、李涛鸣、吴峥、宋士涛、严卫国、石旭、陈建军、陈涛、陈婷婷、杨国军、何易、杨炯光、李继东、蔡朝华、陈青明、周晓荣、吴涛、刘洪、郑维彬、张珑凡、晋新华、杨玉丰、熊燕情、郑成龙、王哲媛、谢幸洋、 陈华、吉国佳、丁锐文、蔡震、曹峰、文利、张强、马华、张茵、韩兴文。

危险化学品数字身份认证通用规范

1 范围

本文件规定了危险化学品数字身份编码及载体、数字身份认证与授权管理、以及实验方法。

本文件适用于危险化学品在生产、存储、运输、经营、使用及销毁全生命周期过程中数字身份的数据解读、授权、核验、鉴证、溯源等活动。

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 42570-2023 信息安全技术 区块链技术安全框架

GB/T 43579-2023 区块链和分布式记账技术 智能合约生命周期管理技术规范

GM/T 0130-2023 基于SM2算法的无证书及隐式证书公钥机制

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字身份 digital identity

主体在互联网中的虚拟身份表示，关联了与该主体相关的属性信息，通常由一个账户标识其唯一性。

[来源：GB/T 31504-2015，3.6]

3.2

授权 authorization

根据对主体数字身份信息的评估，确定一个主体是否可以对资源实施指定类型的访问的过程。一旦某个主体被鉴别，可拥有某些类型的访问权限。

[来源：GB/T 31504-2015，3.5]

3.3

数字身份信息 digital identity information

与数字身份关联的主体相关的属性信息。

[来源：GB/T 31504-2015，3.7]

3.4

数字身份认证 digital identity authentication

通过数字技术手段，对危险化学品及其相关参与方的身份信息进行验证、识别和确认的过程。

3.5

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人(例如接收者)伪造的目的。

[来源：GB/T 25069—2022，3.576]

3.6

载体 carrier

用于承载危险化学品数字身份，具有授权访问机制和密码运算功能的安全芯片。

3.7

有源载体 active carrier

内置电池或能源供应，可主动发射信号、实时通信或动态上报数据。

3.8

无源载体 passive carrier

无需内置电源，通过外部设备（读写器、手机等）的射频信号或光学信号激活，实现数据读取与交互。

3.9

区块链 blockchain

使用密码链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：GB/T 43572-2023，3.6]

3.10

智能合约 smart contract

存储在分布式记账技术系统中的计算机程序,该程序的任何执行结果都记录在分布式账本中。

[来源：GB/T 43572-2023，3.72]

3.11

区块链存证 blockchain preservation

基于区块链技术实现多节点共识的电子数据存证。

[来源：GB/T 43580-2023，3.4]

3.12

存证唯一标识码 unique identifier of preserve evidence

存证信息的唯一标识符号,通常为一组字符串。

[来源：GB/T 43580-2023，3.10]

3.13

危险化学品 hazardous chemicals

具有毒害、腐蚀、爆炸、燃烧、助燃等性质，对人体、设施、环境具有危害的剧毒化学品和其他化学品。

[来源：GB 18218 2018，3.1]

3.14

危险化学品安全信息 hazardous chemicals safety information

危险化学品的名称、危害分类、管控要求、安全操作、应急处置等安全管理相关信息。

3.15

产品信息 production information

危险化学品产品的供应商、种类、批次、包装规格、有效期等相关信息。

3.16

危险化学品安全信息码 hazardous chemicals safety information code

危险化学品登记综合服务系统生成的用于表示化学品危害信息的二维码,编码内容中应包括供应商信息和危险化学品安全信息，可根据企业需求扩展生产批次、包装、有效期等产品信息。

3.17

可追溯性 traceability

追溯客体的历史、应用情况或所处位置的能力。

[来源：GB/T 38155-2019，2.3]

3.18

追溯标签 traceability label

以文字、图形、符号等方式标示追溯码及相关信息的标牌，与所追溯产品具有对应关系。 注：包括印刷标签、电子标签等。

[来源：GB/T 38155-2019，3.17]

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)

Beacon：蓝牙信标（Bluetooth Beacon）

CAS：化学文摘社（Chemical Abstracts Service）

LoRa：长距离无线电（Long Range Radio）

MSDS:化学品安全技术说明书(Material Safety Data Sheet)

NB-IoT：窄带物联网（Narrow Band Internet of Things）

NFC：近场通信（Near Field Communication）

UN编号：联合国危险货物编号（United Nations identification Number）

WIA-FA设备：工业无线网络 工厂自动化（Wireless Network for Industrial Automation－Factory Automation）

5 数字身份编码及载体

5.1 数字身份编码

5.1.1 通则

危险化学品数字身份编码应遵循国家相关法规，核心内容包括物质唯一标识、危险特性分类、企业生产信息、监管合规信息及扩展字段，确保危险化学品全生命周期的可追溯、可监管、可应急响应。在实际应用中，可结合行业需求调整字段的适用范围和优先级，并通过版本控制和扩展预留确保编码规则具有向下兼容和向上扩展的能力，以适应未来监管要求升级。

5.1.2 编码结构

危险化学品编码应采用“前缀和版本码－CAS号－UN编号－危险类别－危险特性－企业代码－生产批次－唯一序列－校验码－扩展字段”的十段式结构，各段含义和结构定义应符合表1的规定。

表1 危险化学品数字身份编码结构及示例

段序	字段名称	长度（位）	说明	示例（苯）
1	前缀和版本码	3	由2位固定前缀加1位版本号组成。前缀固定为“GH”，标识危险化学品专属编码；版本号用于标识编码版本，当前版本为“1”，通过版本控制实现编码规则的升级和兼容。	GH1
2	CAS号	10	物质唯一标识，美国化学文摘登记号（格式：XXXXXXX-XX-X）。为便于处理，可将CAS号中的短横线去除或按固定长度填充。	71-43-2（苯的CAS号）
3	UN编号	5	联合国危险货物编号（格式：“UN”+4位数字）。存储时可仅记录数字部分。	UN1114（苯的UN编号）
4	危险类别	4	危险性质分类编码，对应GB 13690规定的一级分类和二级分类代码（数字组合）。	0301（一级：易燃液体；二级：苯）

5	危险特性	4	基于 GHS（全球化学品统一分类和标签制度）危险性说明的缩写代码，表示主要危险特性。	FLAM（易燃液体）
6	企业代码	4	企业唯一标识代码（可取统一社会信用代码后 4 位或应急管理部门危险化学品备案证书编号后 4 位）。	0012（某企业代码示例）
7	生产批次	10	生产批次信息，建议格式：YYYYMMDDXX，其中 YYYY=年，MM=月，DD=日，XX=当日批次流水号。	2024050101（2024 年 5 月 1 日第 01 批）
8	唯一序列	8	确保编码全局唯一的序列号，由系统生成的随机或递增序列组成（字母数字混合）。	5A8F3B2D
9	校验码	1	根据前若干段的内容计算得到的一位校验数字，用于校验编码有效性。计算时应去除分隔符及非数字字符，采用加权求和取模 10 的方法确定校验码（详见附录 B）。	7
10	扩展字段	4	预留字段，初始填充“0000”。用于未来扩展，如添加新的标识要素或功能码，以增强编码表达能力。	0000
注1：当编码规则需升级时，可通过提高版本号或利用扩展字段增加新元素，从而保证新版本编码与旧版本编码的兼容识读。 **注2：**危险化学品数字身份编码与数字证书信息相互映射：数字证书中包含的与编码各字段对应的关键属性应符合附录A和附录B规定，确保实体标签编码与链上身份数据的一一对应关系。 **示例：**以某化工企业生产的 2024 年第 1 批苯（CAS 号 71-43-2，UN 编号 1114，危险类别代码 0301，主要危险特性 FLAM，企业代码 0012）为例，其危险化学品数字身份完整编码如下： GH1-71432-UN1114-0301-FLAM-0012-2024050101-5A8F3B2D-7-0000				

5.2 数字身份载体

5.2.1 有源载体

5.2.1.1 蓝牙低功耗信标（Beacon）模块

内置电池，定期广播身份标识，应支持短距离定位与状态上报；可通过动态密钥实现加密通信。

5.2.1.2 北斗模块

集成北斗卫星定位功能的电子标签装置，主要技术要求如下：

a) 轨迹记录：可记录并实时上传定位轨迹；
b) 高精度授时：利用卫星授时，可在上传数据时添加高精度时间戳（如北斗时，误差≤10 ns）；
c) 地理围栏：支持设置地理围栏认证，当载体位置信息超出授权范围时应触发告警。

5.2.1.3 NB-IoT/LoRa 设备

内置窄带物联网或长距离无线通信模块的标签，具备远程广域通信能力。主要技术要求如下：

a) 可定期上报温度、湿度、压力等环境参数，实现远程监控；
b) 设备支持远程固件升级且需通过数字签名验证确保固件来源可信。

5.2.1.4 WIA-FA 设备

符合工业无线网络工厂自动化标准的工业级无线通信装置。

a) 高性能通信:具有微秒级低时延（≤10 ms）和高可靠性（丢包率<0.1%）的特性；
b) 身份鉴权:WIA-FA 载体应进行设备身份鉴权和通信加密认证，接入网络前通过预共享密钥与认证服务器双向鉴别身份；
c) 加密认证:通信过程中宜采用国密 SM4 或 AES-128 算法对数据帧加密，并附加序列号与 CRC 校验码，接收方验证序列号连续性和 CRC 以确保数据完整及来源可信。

5.2.2 无源载体

5.2.2.1 RFID 标签

超高频无源射频识别（Radio Frequency Identification，RFID）标签，内含天线和芯片，无需电池，依靠读写器射频信号供能并传输数据。芯片可存储危险化学品数字身份的基础标识数据。

读取时通过射频获取标签内信息，实现静态编码认证，并可利用标签内置的存储和密码功能对读取权限进行简单控制。

5.2.2.2 二维码/条形码

二维码/条形码是基于光学识读的平面编码载体，可作为辅助标识。

读取时通过扫码设备获取编码信息，系统可调用区块链或数据库验证二维码/条形码内容的真实性。

5.2.2.3 NFC 标签

NFC标签是近场通信标签，无源供电，利用13.56MHz射频场与读取设备（如智能手机）通信。

NFC载体可存储数字身份认证所需的证书哈希或密钥索引，当终端设备贴近时应触发双向认证过程：读取设备与标签进行一次握手协商，验证标签内信息与后端数据源一致性。

6 数字身份认证与授权管理

6.1 概述

危险化学品数字身份认证平台（以下简称“平台”）基于区块链技术与权限管理，实现了对危险化学品全生命周期各环节数据的采集、验证与共享，具体流程见图1。平台运用数字证书、加密技术和智能合约，确保身份数据的真实、完整与可追溯，并通过授权机制管理数据访问。密码体系以国密算法为核心，兼容国际算法，并支持未来扩展。

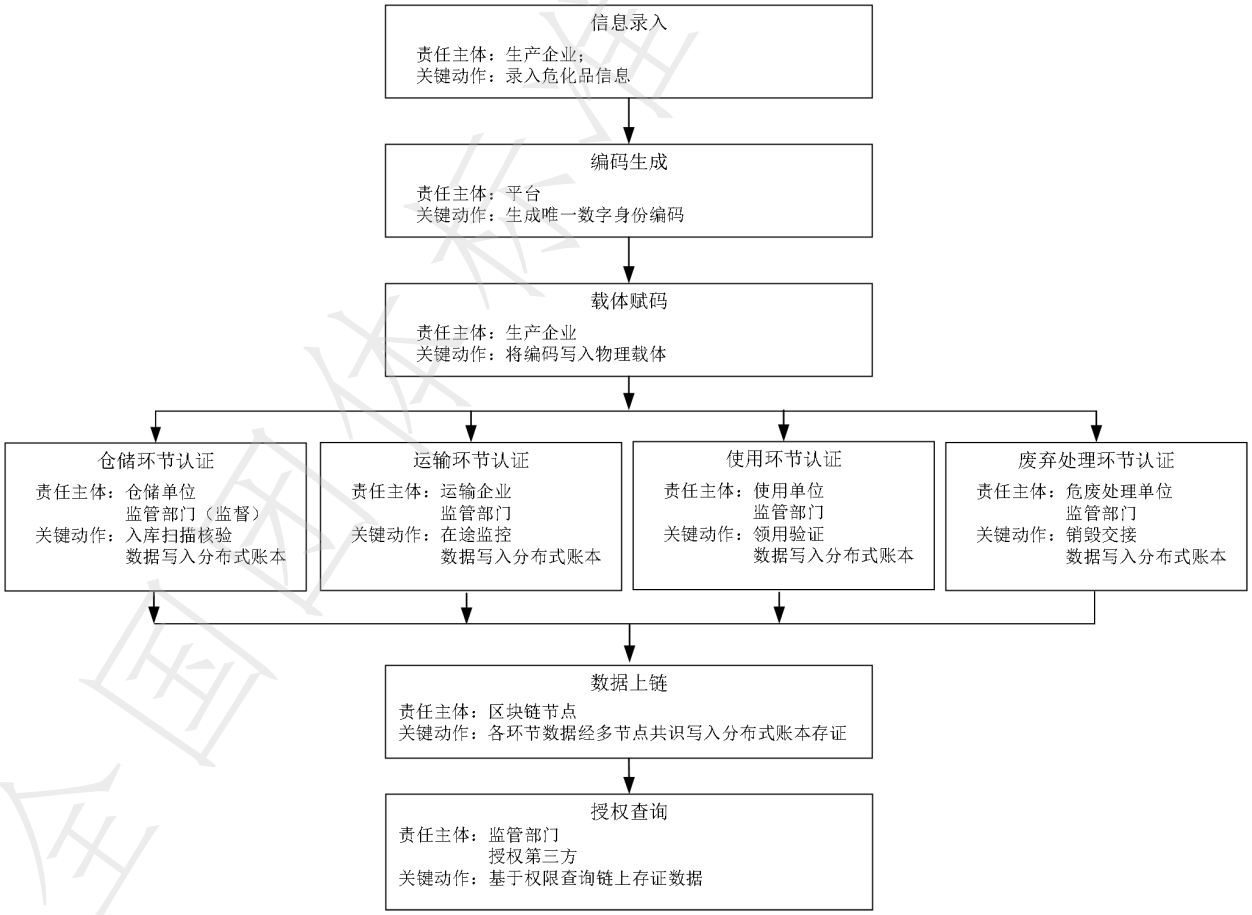

图 1 危险化学品数字身份全生命周期流程示意

6.2 认证方式

6.2.1 有源载体

6.2.1.1 主动数据上报

周期性主动发送包含自身身份标识和状态的数据包至平台，由平台验证数据的完整性和时序，实时监控危险化学品状态。

6.2.1.2 挑战-响应鉴别

有源载体与认证服务器之间可采用挑战/响应协议进行双向鉴别。载体发送包含设备ID和随机数的认证请求，服务器返回挑战值，载体使用预置密钥对随机数和挑战值加密后回传。服务器解密验证，以确认载体为合法设备，防止伪冒接入。

6.2.1.3 通信链路加密

有源载体和读取/接收设备之间的通信应全程加密。宜采用国家密码算法（如SM4）或兼容的AES-128算法对传输的数据帧加密，同时加入防重放的序列号和防篡改的校验码。

6.2.1.4 动态密钥和时间戳

为提高认证可靠性，有源载体可结合动态密钥或时间戳技术，有源载体数字身份认证时序见图2。

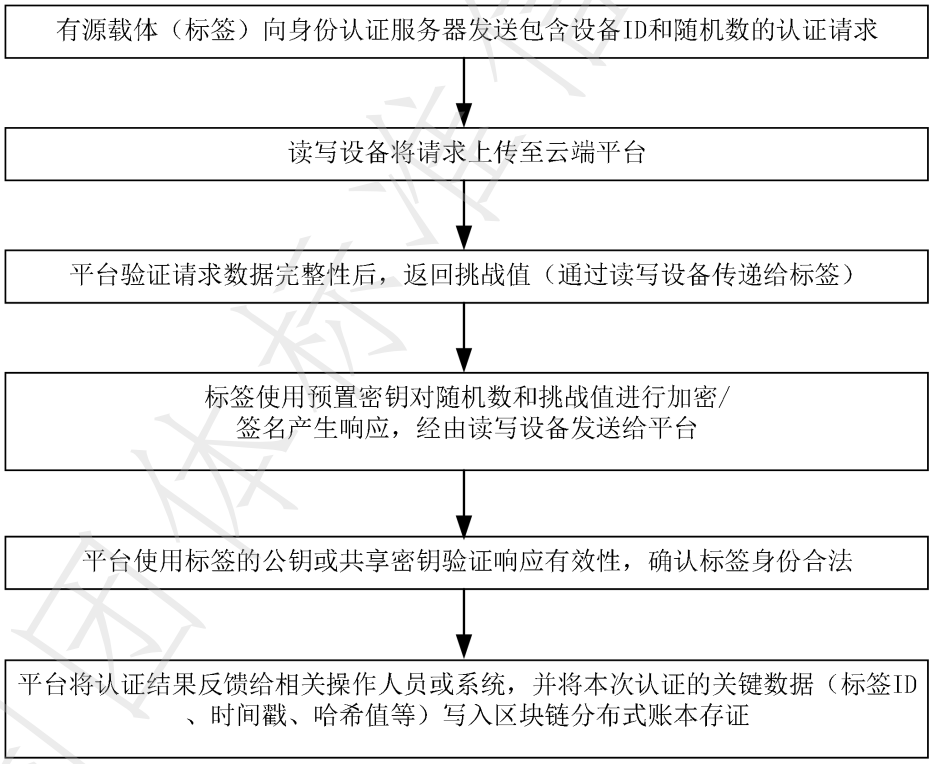

图 2　有源载体数字身份认证时序图

6.2.2 无源载体

6.2.2.1 静态数据校验

对于RFID、条码等被动标签，读取设备获取标签存储的身份编码后，提交给平台或本地校验系统进行比对。系统从区块链中查询对应危险化学品的登记信息，核实标签读取的数据真实性和完整性。

6.2.2.2 防伪查询

针对印刷二维码等易复制的载体，可通过联网查询验证真伪。此过程宜对用户透明，即用户扫码即可获得“验证通过”或警示信息。

6.2.2.3 近场双向认证

NFC类标签支持短距离交互，可设计简化的双向认证流程。

6.3 授权流程

6.3.1 初始授权

用户提交资质材料完成注册，平台审核通过后颁发数字身份和数字证书，按角色分配初始权限。

6.3.2 数据存证授权

具有数据存证职能的危险化学品生产企业等用户，可向平台申请获取存证权限及密钥对；经审批通过后，用户可上传业务数据并进行数字签名认证，生成数字身份编码及证书后上链存证。

6.3.3 数据监管授权

监管用户经资质审核通过后，获得相应权限，可查看授权范围内的危险化学品全生命周期数据。监管用户仅可对数据进行查阅或导出，不应进行修改。

6.3.4 数据使用授权

科研机构、应急处置部门等数据使用用户提交数据使用申请后，经平台审核通过，授予数据使用密钥。该密钥仅限在授权范围内使用，且使用行为应受平台监控。

6.3.5 第三方数据共享授权

第三方提交共享请求，平台审核并签订协议后，通过智能合约授予查询权限，共享过程留痕可追溯，权限可随时终止。数据共享授权流程见图3。

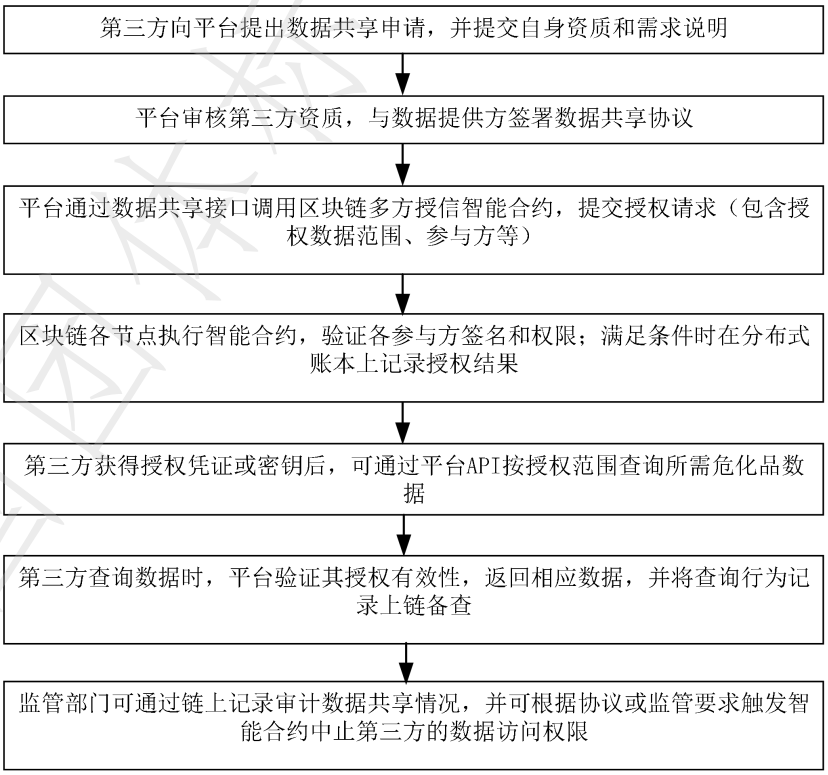

图 3 第三方数据共享授权流程

6.3.6 第三方共享的智能合约

智能合约遵循“最小上链、职责分离、可撤销授权、可审计”的原则，接口应符合GB/T 43579-2023、GB/T 42570-2023的要求，具体调用授权流程见图4。

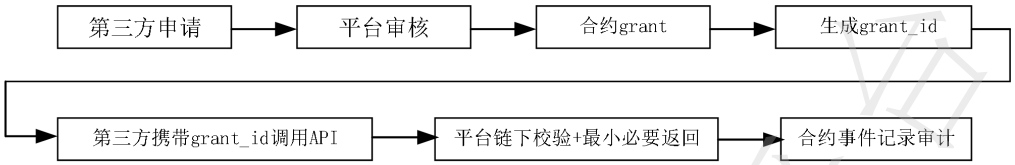

图 4　智能合约调用授权流程

6.4　有源载体全流程认证

6.4.1　危险化学品信息录入与标签生成

生产企业录入危险化学品名称、主要成分及物理化学性质、危险类别、生产日期、批次号、有效期、储存要求等详细信息和企业资质信息，平台依据第5章生成唯一数字身份编码和存证，签发数字证书并写入有源标签。

6.4.2　有源载体安装与初始化

标签安装于包装容器或储运装置，进行配置通信参数、校准集成传感器等初始化操作。将标签ID与该批危险化学品的数据记录绑定，验证其通信与认证功能正常后，正式启用该危险化学品的数字身份。

6.4.3　仓储环节认证

危险化学品入库时，入口读写设备应自动读取有源标签身份数据，并进行品名、批次、数量、存放区域等信息对比，入库操作数据（时间、地点、经手人、货位）应上链存证。

仓储期间，应实时监测环境参数，定期上传平台并上链，若发现异常，应立即告警并上链记录；管理人员应定期扫描标签进行盘点，核对实际存放情况与链上记录是否一致。

所有入库、监测、异常处理操作均应与数字身份关联留痕，供监管方查询核验。

6.4.4　运输环节认证

危险化学品出库装车前，运输人员应读取有源标签，确认货物、运单信息和承运资质，并在平台录入车辆、司机、路线等运输信息，与化学品数字身份关联上链，形成运输任务记录。

运输途中，应定时读取货物状态（如温度、压力）及车辆实时位置，并上传至平台。若出现车辆偏离路线、长时间停滞或货物参数异常，平台应自动预警并通知相关方，智能合约同步将异常信息上链。

运抵目的地后，收货方应读取标签核对运输记录与货物状态，确认无误后在平台完成签收。平台应对交付记录加盖时间戳永久保存，更新化学品状态为“已交付”，并通知发货方与监管部门。

6.4.5　使用环节认证

使用单位领取危险化学品时，应通过读取有源标签验证使用资质与权限，通过后方可领取，同时应将领取时间、数量及用途等信息上链记录，形成授权凭证。

使用过程中，使用单位应按规定管理，定期向平台上报使用时间、用量、操作人、剩余库存等关键数据。所有使用记录均应上链保存。

6.4.6　废弃处理环节认证

危险化学品需废弃时，使用单位应在平台提交处置申请，经监管部门审批后由专业危废单位处理。回收时，处理方扫描标签核对化学品信息，平台验证其与链上记录一致后，完成交接并上链。

处置过程中，处理方法、时间、经办人等关键数据实时上传至区块链，形成完整处置记录。销毁完成后，平台将该化学品数字身份状态更新为“已销毁”，并生成区块链存储的销毁证书。

6.5　无源载体认证

6.5.1　信息上链与数字身份生成

6.5.1.1　危险化学品信息登记

生产企业在每批危险化学品生产完成后，应记录该批次危险化学品名称、化学成分、物理特性、危险等级、生产批次、生产日期、有效期等产品信息，以及企业的生产许可证、产品合格证明等资质材料。

6.5.1.2 区块链登记

生产企业将6.5.1.1记录的信息录入危险化学品数字身份认证平台。

平台生成唯一的数字身份标识（编码），并将编码与危险化学品信息、企业信息记录在区块链中，生成该批危险化学品的数字身份链上档案。

6.5.1.3 数字身份生成

平台根据链上存证信息，签发对应的危险化学品数字身份证书，内容涵盖企业主体、危险化学品详细信息、数字身份编码及证书有效期等，宜通过国家密码算法对证书签名。

数字身份证书可供企业下载保存，也可用于验证。

6.5.2 无源载体关联与标记

6.5.2.1 选择载体类型

企业应根据危险化学品包装形式和使用环境选择合适的无源标签作为身份载体。

6.5.2.2 写入身份信息

平台将生成的数字身份编码通过特定方式写入无源载体，具体流程见图5。

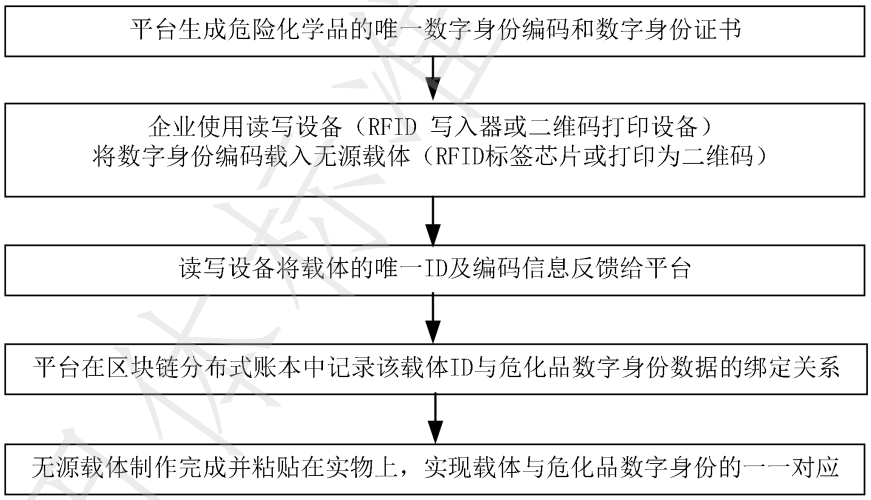

图 5 无源载体关联赋码流程

6.5.3 仓储环节认证

危险化学品运抵仓库入库时，管理人员应读取无源标签，具体流程和要求见5.4.3。

6.5.4 运输环节认证

危险化学品出库装车前，运输人员应读取无源标签，具体流程和要求见5.4.4。

6.5.5 使用环节认证

危险化学品被使用单位领取时，应通过扫描无源标签在平台提交申请，具体流程和要求见5.4.5。

6.5.6 废弃处理环节认证

见6.4.6。

7 实验方法

7.1 实验原理

危险化学品数字身份认证实验应利用密码算法和标准化的编码/证书体系，通过对危险化学品的数字身份进行读取、验证和比对，以评估平台在真实性校验、异常检测方面的性能，主要技术架构包括：

a) 数字身份证书：采用国家密码算法（如 SM2/SM3/SM4）生成包含化学品编码、企业信息与公钥的数字证书，用于身份验证，并通过加密保障传输安全。
b) 无源载体认证机制：标签存储身份编码或证书哈希值。读取后，平台通过国密算法校验哈希，比对区块链存储值，确保数据完整、未经篡改。
c) 有源载体认证机制：标签内置安全芯片和密钥，与服务器进行双向身份认证，并可通过临时密钥建立加密通信通道。
d) 区块链存证与触发：所有关键身份数据、操作日志及异常事件均上链存储。智能合约按规则自动监控，发现违规或危险时触发告警，确保记录不可篡改、全程可溯。

7.2 实验设备与试剂

7.2.1 设备清单

实验所需的主要设备如表2所示。

表 2 危险化学品数字身份认证实验设备清单

序号	设备类别	无源认证	有源认证
1	标识载体	防伪二维码标签、UHF RFID 电子标签	BLE 蓝牙低功耗标签、LoRa 无线标签
2	读写设备	二维码扫描仪、RFID 读写器	蓝牙网关、LoRa 网关
3	加密模块	国密加密芯片（集成于读写器）	国密安全芯片（嵌入于有源标签）
4	后台服务器	危险化学品数字身份认证平台服务器	边缘计算网关（支持动态密钥协商）
5	网络设备	RFID 信号放大器	LoRa 基站、Wi-Fi 路由器

7.2.2 试剂与材料

实验涉及的标签介质及化学品样本如表3所示。

表 3 危险化学品数字身份认证实验所需材料

序号	材料类别	无源认证材料	有源认证材料
1	物理标识介质	聚丙烯材质防伪二维码标签	环保 PC 材质电子标签（内置 BLE/LoRa 模块）
2	化学品样本	硝酸铵、浓硫酸等（危险样品）	（使用相同样本，仅区分载体类型）
3	安全存储介质	USB 安全钥匙（存储私钥）	动态令牌设备（用于生成一次性密钥）

7.3 实验步骤

7.3.1 无源载体认证实验

无源载体认证实验步骤如下：

a) 标签初始化：宜使用支持国密算法的读写器，将危险化学品的数字身份编码及对应证书哈希值写入 RFID 标签或生成二维码标签，确保与区块链平台原始信息一致；
b) 数据关联：在平台中将标签 ID 与该危险化学品的数据条目绑定，建立一一对应关系；
c) 身份核验测试：依次进行下列操作验证无源标签的身份认证效果。
   1) 使用扫描设备读取标签中的危险化学品编码。
   2) 平台校验编码有效性，并比对标签哈希值与链上存证的哈希值。
   3) 平台验证区块链中该化学品数字身份证书的签名与状态，向终端返回认证结果。

7.3.2 有源载体认证实验

有源载体认证实验步骤如下：

a) 终端配置进行的操作如下：

1） 配置符合国密标准的有源标签，预先写入平台颁发的数字证书与密钥，确保能与边缘网关/服务器正常通信。
2） 准备动态令牌设备，用于生成认证所需的挑战随机数。

b） 双向认证测试进行的操作如下：
1） 模拟有源标签与服务器的双向鉴别和数据上报：
2） 标签向服务器发送含自身标识和时间戳的认证请求；
3） 服务器对响应数据签名或加密后返回，标签验证服务器身份；
4） 标签生成模拟传感数据（如温度）并签名，通过网关上报平台；
5） 平台验证签名后，将数据及验证结果写入区块链，并更新该化学品数字证书状态。

注：在双向认证测试过程中监测：终端是否能正确识别服务器身份，服务器能否验证终端签名数据的真实性，以及区块链是否成功记录本次认证交互日志。

7.4 质量控制

7.4.1 设备校准

在实验开始前应对所有读写设备进行校准。

7.4.2 区块链一致性验证

测试区块链在异常情况下的数据可靠性。

模拟部分节点离线或网络延迟的情形，检查剩余节点能否正常达成共识、生成区块，以及恢复后的节点能正确同步数据。

通过比对不同节点对同一数据的区块哈希值是否一致，验证区块链存证的不可篡改性和容错性。

7.4.3 数据备份

为防止意外情况导致实验数据丢失，应建立区块链数据和实验记录的备份机制。对链上数据每日进行增量备份，对关键实验日志另存档备案。

7.4.4 外部质量评估

宜邀请具有资质的第三方检测机构对实验过程和结果进行评估，或参与实验室间比对测试。

7.4.5 人员培训与考核

对实验人员进行专业培训，确保其熟悉实验步骤、设备操作和安全注意事项，并定期进行考核。

7.5 数据处理与报告

7.5.1 数据记录

认真记录实验过程中的所有数据，包括读取到的数字身份信息、比对结果、检测结果等。

7.5.2 数据处理

对记录的数据进行必要的处理和分析，如数据清洗、统计和计算等。

7.5.3 报告编制

将实验结果整理成详细的实验报告，包括实验目的、步骤、结果、结论等，并附上必要的图表和数据。

附 录 A
（规范性）
数字证书管理流程

A.1 数字证书格式

危险化学品数字身份证书采用数字证书的通用格式（如X.509 v3标准）或等效的国密证书格式。证书内容包含如下主要字段：

a) 版本号：标明证书格式版本，例如 X.509 第 3 版。
b) 证书序列号：由签发机构分配的唯一序列码，可采用危险化学品数字身份编码或其哈希作为序列号的一部分，确保证书与对应危险化学品一一对应。
c) 签名算法标识：用于签发证书的数字签名算法标识，如 SM2 with SM3（表示采用 SM2 算法对证书内容的 SM3 哈希签名）。
d) 颁发者信息：签发该证书的机构标识信息，例如“CN=危险化学品数字身份认证平台 CA，OU=数字身份管理中心，O=中国移动通信联合会”等。
e) 有效期：证书的起始生效时间和失效时间。对于危险化学品证书，可根据危险化学品生命周期或企业资质有效期设置证书有效期限，并可在到期前更新。
f) 使用者（主体）信息：证书持有者信息，包括危险化学品及相关企业的标识。例如，“CN=苯_2024 第 1 批，O=某化工企业，L=生产场所地址”等，也可在证书 Subject 的扩展字段中加入危险化学品唯一编码、CAS 号、企业代码等，以清晰标识证书所对应的具体危险化学品实体。
g) 主体公钥信息：证书持有者的公钥值及其算法参数。对于隐式证书方案，则存储由主体标识计算得到的公钥或相关参数（参见 GM/T 0130-2023）。
h) 扩展字段：根据需要添加的附加信息。扩展字段应使用证书扩展格式标记为非关键项，供平台和监管系统解析使用。

A.2 数字证书管理

A.2.1 数字证书申请和生成

企业在危险化学品数字身份认证平台提交营业执照、许可证等资质文件，平台审核通过后，为其生成企业身份数字证书。

企业可在平台提交具体危险化学品信息。平台将信息进行区块链存证并生成唯一编码，据此签发包含企业及化学品详细信息的危险化学品数字证书。

A.2.2 数字证书下载与查询

证书生成后，平台通知企业下载。企业登录后可下载数字证书，并应将其保存至安全存储介质中。

用户、监管部门或授权供应链企业均可通过扫描数字证书或在平台输入危险化学品编码，查询危险化学品相关存证信息及全生命周期数据。

A.2.3 数字证书更新与撤销

危险化学品企业的相关信息、经营业务等发生变化时，危险化学品企业应上报更新内容，重新个性化载体，更新数字证书。当经营范围变化或因其它原因需撤销证书时，应清除载体存储的数字证书信息。

附 录 B
（规范性）
数据字段及编码结构对照

B.1 数字身份编码字段映射

危险化学品数字身份编码各段字段的来源或依据，以及在数字证书和监管数据中的体现见表B.1。

表 B.1 危险化学品数字身份编码字段映射关系

字段名称	映射/来源依据	与数字证书及系统数据的关系
前缀和版本码	前缀“GH”规定危险化学品类别，版本码由本标准定义	证书序列号或扩展字段中包含版本信息，用于兼容性识别
CAS 号	化学品登记号，来源于 CAS 注册数据库	证书主题或扩展字段中记录 CAS 号，唯一标识化学品
UN 编号	联合国危险货物编号，依据联合国《关于危险货物运输的建议书》	证书扩展字段中可含 UN 编号，用于运输监管的数据关联
危险类别	危险物质分类代码，依据 GB 13690 等国家标准	证书主题中可体现主要危险类别；链上存证包含该分类信息
危险特性代码	GHS 危险性说明缩写，依据联合国 GHS 标准和行业惯例	证书扩展字段记录主要危险属性；提供应急处置参考
企业代码	企业标识代码，取自企业统一社会信用代码或备案登记编号	证书主题中包含企业名称/代码；链上关联企业资质存证
生产批次	企业自定批次号，格式 YYYYMMDDXX，本标准规定格式	证书扩展字段可记录生产批次；链上存证详细追溯该批次信息
唯一序列	由平台生成的随机/顺序号，保证编码全局唯一	用于证书序列号或哈希计算的一部分，防止重复
校验码	根据上述字段按算法计算生成，防误读校验	不直接存储于证书；扫描时由系统重新计算比对验证
扩展字段	预留扩展信息，目前填充“0000”	证书可包含对应的扩展 OID；未来用于新字段兼容扩展

B.2 校验码计算规则

危险化学品数字身份编码的校验码用于快速验证编码输入的准确性，防止常见错误（如字符遗漏或替换）。校验码的计算采用加权求和取模 10 的方法，具体规则如下：

a) 选取字符：取编码字符串中除校验码段以外的所有字符，去除分隔符“-”以及字母字符，仅保留数字字符参与校验计算。
b) 示例：对于示例编码“GH1-71432-UN1114-0301-FLAM-0012-2024050101-5A8F3B2D-7-0000”，去除非数字和分隔符后得到的数字串为：17143211140301001220240501015。
c) 设置权重：根据字符在数字串中的位置赋予不同权重值。
d) 计算求和：将每个位置上的数字乘以该位置的权重，再求所有乘积的和，得到总和值 S。
e) 取模求余：计算 S 除以 10 的余数 r（r = S mod 10）。
f) 确定校验码：将余数 r（若为 0 则校验码为 0）作为校验码，插入编码末位。
g) 校验码验证：读取编码后，提取末位校验码，对前面部分按相同规则重新计算余数 r′，若 r′ 与提取的校验码一致，则校验通过。

参 考 文 献

[1] GB 13690-2009 化学品分类和危险性公示 通则
[2] GB/T 17902.2-2005 信息技术 安全技术 带附录的数字签名 第2部分:基于身份的机制
[3] GB/T 25069-2022 信息安全技术 术语
[4] GB/T 31504-2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范
[5] GB/T 32905-2016 信息安全技术 SM3密码杂凑算法
[6] GB/T 32907-2016 信息安全技术 SM4分组密码算法
[7] GB/T 35276-2017 信息安全技术 SM2密码算法使用规范
[8] GB/T 38155-2019 重要产品追溯 追溯术语
[9] GB/T 38629-2020 信息安全技术 签名验签服务器技术规范
[10]GB/T 42474.1-2023 爆炸危险化学品汽车运输安全监控系统 第1部分：通用技术要求
[11]GB/T 42571-2023 信息安全技术 区块链信息服务安全规范
[12]GB/T 42752-2023 区块链和分布式记账技术 参考架构
[13]GB/T 43572-2023 区块链和分布式记账技术 术语
[14]GB/T 43575-2023 区块链和分布式记账技术 系统测试规范
[15]GB/T 43580-2023 区块链和分布式记账技术 存证通用服务指南
[16]GB/T 43582-2023 区块链和分布式记账技术 应用程序接口 中间件技术指南
[17] GB/Z 24294.3-2017信息安全技术 基于互联网电子政务信息安全实施指南 第3部分：身份认证与授权管理
[18]GM/T 0010-2023 SM2密码算法加密签名消息语法规范
[19]JT/T 1386.10-2022 海事电子证照 第10部分：危险化学品水路运输从业资格证书
[20]JT/T 1385.12-2023 水路运输电子证照 第12部分：危险化学品水路运输从业资格证书
[21]YD/T 4598.6-2024 面向云计算的零信任体系 第6部分：数字身份安全能力要求
[22]危险化学品目录（2015版）