ICS 35.040
CCS A 24

DB37

山　东　省　地　方　标　准

DB37/T 4811.2—2025

工业互联网标识解析　仪器仪表
第2部分：应用服务平台接口规范

Identification and resolution system for the industrial internet—Measuring instruments—Part 2:Application service platform interface specifications

2025－02－14 发布　　2025－03－14 实施

山东省市场监督管理局　　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。

本文件是DB37/T4811《工业互联网标识解析　仪器仪表》的第2部分。DB37/T4811已经发布了以下部分：

——第 1 部分：被动标识载体应用指南；

——第 2 部分：应用服务平台接口规范；

——第 3 部分：应用服务平台数据元规范；

——第 4 部分：应用服务平台运营规范。

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。

本文件由山东省工业和信息化厅提出、归口并组织实施。

引　言

推动工业互联网标识解析的应用，是构建工业互联网生态，促进新一代信息技术与工业经济深度融合的重要环节和抓手，是实现经济社会中人、企业、设备、系统、数据互联互通的重要基础。

为进一步促进仪器仪表行业工业互联网应用，DB37/T 4811《工业互联网标识解析　仪器仪表》为工业互联网标识解析仪器仪表应用服务平台建设提供了重要基础支撑。DB37/T 4811拟由四个部分组成。

——第1部分：被动标识载体应用指南。目的在于为工业互联网标识解析仪器仪表标识载体应用提供指导。

——第2部分：应用服务平台接口规范。目的在于为工业互联网标识解析仪器仪表应用服务平台接口确立相关规范。

——第3部分：应用服务平台数据元规范。目的在于为工业互联网标识解析仪器仪表应用服务平台数据元确立相关规范。

——第4部分：应用服务平台运营规范。目的在于为工业互联网标识解析仪器仪表应用服务平台运营确立相关规范。

工业互联网标识解析　仪器仪表　第2部分：应用服务平台接口规范

1　范围

本文件规定了工业互联网标识解析仪器仪表应用服务平台接口设计、接口分类、接口技术、接口开发、接口使用和接口安全等方面的要求，描述了对应的证实方法。

本文件适用于工业互联网标识解析仪器仪表应用服务平台能力建设及应用。

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 15843.3—2023　信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制

GB/T 15851.3—2018　信息技术　安全技术　带消息恢复的数字签名方案　第3部分：基于离散对数的机制

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

GB/T 35273—2020　信息安全技术　个人信息安全规范

DB37/T 3523.2—2019　公共数据开放　第2部分：数据脱敏指南

3　术语和定义

下列术语和定义适用于本文件。

3.1

令牌　token

通过应用服务平台登录认证后生成，用于标识用户的登录身份信息。

3.2

客户　customer

完成应用服务平台注册并通过审核的自然人或法人主体。

3.3

身份认证　identity authentication

对自然人的身份进行确认。

注：身份认证包含登录认证和实名核验。

4　缩略语

下列缩略语适用于本文件。

AMQP：高级消息队列协议（Advanced Message Queuing Protocol）

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

App：应用程序（Application）
AppKey：应用密钥（Application Key）
CPU：中央处理器（Central Processing Unit）
HTTP：超文本传输协议（Hypertext Transfer Protocol）
HTTPS：安全超文本传输协议（Hypertext Transfer Protocol Secure）
MQTT：消息队列遥测传输协议（Message Queuing Telemetry Transport）
SDK：软件开发工具包（Software Development Kit）
URL：统一资源定位符（Uniform Resource Locator）

5 接口设计

接口设计应包括但不限于以下内容。

a) 安全性：提供多种安全可靠的技术手段，保证服务接口的安全。
b) 开放性：采用通用的接口设计标准，保证与其他系统的互联互通。
c) 灵活性：能根据业务变化，灵活调整接口容量与性能。

6 接口分类

6.1 概述

工业互联网标识解析仪器仪表应用服务平台应对外提供安全类接口、数据类接口、服务类接口和应用类接口以及标识类接口、事件类接口和运行类接口。应用服务平台接口分类见图1。

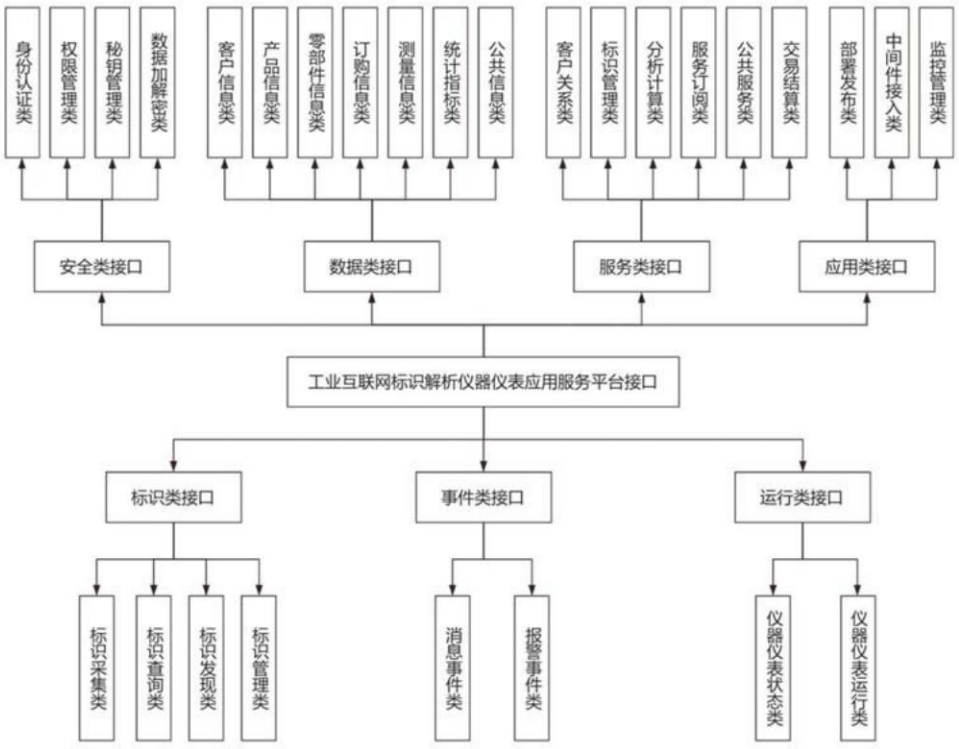

图1 接口分类

6.2 安全类接口

安全类接口应包含但不限于以下类型。

a) 身份认证类：包含自然人认证（用户名/密码、手机短信、第三方认证）、接口 API 认证等接口。
b) 权限管理类：包含获取权限、授予权限、删除权限等接口。
c) 密钥管理类：包含密钥上传、密钥删除等接口。
d) 数据加解密类：包含数据加密、数据解密等接口。

6.3 数据类接口

数据类接口应包含但不限于以下类型。

a) 客户信息类：包含获取客户资料信息、获取客户认证信息、获取 APP 认证信息、获取合作伙伴信息、会员信息、反馈信息等接口。
b) 产品信息类：包含获取仪器仪表基本信息、获取仪器仪表详细信息、仪器仪表分类信息、获取仪器仪表评价信息等接口。
c) 零部件信息类：包含获取产品零件信息、获取产品部件信息、获取产品原材料信息、获取零部件分类信息等接口。
d) 订购信息类：包含获取商品信息、获取商品订单信息、获取账单信息、获取合约信息、获取结算分成信息、获取积分信息等接口。
e) 测量信息类：包含获取仪器仪表测点信息、获取仪器仪表设备信息、获取仪器仪表位置信息、获取企业网关信息、获取采集点信息等接口。
f) 统计指标类：包含获取标识注册量信息、获取测量数据报送指标信息、获取服务使用记录统计信息等接口。
g) 公共信息类：包含获取企业单位类型字典信息、获取企业证件字典信息、获取行政区划编码信息、国家统计局行政管辖区信息等接口。

6.4 服务类接口

服务类接口应包含但不限于以下类型。

a) 客户关系类：包含自然人新增服务、企业信息注册服务、企业信息变更服务、服务提供商注册服务、服务提供商信息变更服务等接口。
b) 标识管理类：包含标识注册服务、标识编码服务、标识赋码服务、标识溯源服务等接口。
c) 分析计算类：包含客户分析评价服务、产品分析评价服务、仪器仪表测量类数据分析服务、仪器仪表全周期视图等接口。
d) 服务订阅类：包含服务发布、服务订阅、服务授权、订单服务等接口。
e) 公共服务类：包含资源上传下载服务、仪器仪表分类更新服务、零部件分配服务、数据采集服务、数据存储服务、数据处理服务等接口。
f) 交易结算类：包含商品交易或服务结算、票据信息等接口。

6.5 应用类接口

应用类接口应包含但不限于以下类型。

a) 部署发布类：包含应用创建、应用上传、服务绑定、服务解绑、应用启动、应用实例数设置、应用动态伸缩设置、应用停止、获取域名详情、绑定域名、解绑域名、应用销毁等接口。
b) 中间件接入类：包含服务接入、创建服务实例、服务实例配置、获取环境变量、删除服务实例、

获取服务实例状态等接口。

c) 监控管理类：包含查看应用流量、查看应用访问量、查看应用 CPU、查看应用内存、监控报警设置等接口。

6.6 标识类接口

标识类接口应包含标识采集类接口、标识查询类接口、标识发现类接口以及标识管理类接口，具体内容如下。

a) 标识采集类：包含仪器仪表标识编码的生成、标识数据的采集，以及向标识解析节点发起的注册登记业务。

b) 标识查询类：包含标识解析，给出仪器仪表产品在制造、销售、检验、使用和计量、管理过程中产生的数据。

c) 标识发现类：根据指定条件查询相关的工业互联网标识解析信息服务的功能。

d) 标识管理类：包含标识的更新、删除以及备份等接口。

6.7 事件类接口

事件类接口应包含消息事件类、报警事件类接口，具体内容如下。

a) 消息事件类：包含编码事件、生产事件、调试事件、流通事件、安装事件、检校事件、维修事件和报废事件等接口。

b) 报警事件类：包含报警事件创建、报警事件设置、获取报警事件、报警事件删除、报警事件触发等接口。

6.8 运行类接口

运行类接口应包含仪器仪表状态类、仪器仪表运行类接口，具体内容如下。

a) 仪器仪表状态类：包含仪器仪表运行时间、获取仪器仪表当前计量、检校状态等接口。

b) 仪器仪表运行类：包含仪器仪表运行数据采集等接口。

7 接口技术

接口技术要求应包括但不限于以下内容。

a) 接口传输协议：支持 HTTPS、MQTT 和 AMQP 等协议中的一种或多种。

b) 接口请求方式：

1) 支持创建资源、获取资源、更新资源、删除资源 4 种操作方式；

2) 采用 HTTPS 协议时应使用标准的 HTTP 请求方法。

c) 支持跨编程语言、跨操作系统调用。

d) 通过应用服务平台分配的接口密钥、访问令牌等方式对调用服务申请进行授权验证。

8 接口开发

接口开发要求应包括但不限于以下内容。

a) 接口描述：描述出接口的概要信息。

b) URL 格式：域名＋/API＋/版本号＋/业务标识。

c) 输入参数：给出参数名称、数据类型、参数值、是否必填等输入信息。

d) 返回参数：给出参数名称、数据类型、是否必填、备注等输出信息。

9 接口使用

工业互联网标识解析仪器仪表应用服务平台使用时，应按照接口调用流程进行企业注册，上传相关材料，经平台运营方审核通过后，为使用方授权认证信息，使用方获取的信息不应泄露给第三方使用。工业互联网标识解析仪器仪表应用服务平台接口调用具体流程见图2，主要包括：

a) 用户登录应用服务平台进行企业注册，等待平台运营方审核；
b) 审核通过后，客户进入平台开发者中心选择对应接口服务目录申请 AppKey；
c) 应用服务平台为客户分配对应的 AppKey 及密钥；
d) 客户进入平台开发者中心查询接口服务目录，并下载接口签名 SDK 包；
e) 客户根据 AppKey 及密钥调用平台 API 认证接口或使用 SDK 包，获取访问令牌；
f) 客户根据访问令牌及生成的签名调用平台接口，或使用 SDK 包访问平台接口。

图2 接口调用流程

10 接口安全

接口相关安全要求应符合GB/T 35273—2020、GB/T 22239—2019、DB37/T 3523.2—2019、GB/T 15851.3—2018、GB/T 15843.3—2023的相关规定。

11 证实方法

11.1 接口分类证实

11.1.1 检查平台的技术文档、API 文档或用户手册，确认是否明确列出了这些接口及其功能描述。
11.1.2 实际调用每个接口，验证它们的响应是否符合预期。
11.1.3 审查平台的源代码，查看是否有实现这些接口的相关代码。

11.2 接口技术证实

11.2.1 检查平台的 API 文档或技术规格说明书，确认其支持的接口传输协议。实际测试调用这些接口，验证它们是否按预期工作。
11.2.2 编写自动化测试脚本，分别测试四种 HTTP 请求方法（POST、GET、PUT、DELETE），确保每种请求均得到正确响应。

11.2.3 使用不同编程语言编写客户端代码，尝试调用平台提供的接口；在不同操作系统上部署并运行这些客户端，接口调用成功且结果一致。

11.2.4 获取接口密钥或访问令牌，观察接口响应，确认是否需要有效的授权信息才能访问接口，并验证授权失败时的返回结果是否符合预期。

11.3 接口开发证实

11.3.1 检查 API 文档或技术规格说明书，确认其中是否包含对接口功能的详细描述。

11.3.2 检查 API 文档中的 URL 示例，确认是否符合规定的格式。

11.3.3 查阅 API 文档中的输入参数部分，确认每个参数的名称、数据类型、默认值（如果有）以及是否为必需参数。

11.3.4 审查 API 文档中的返回参数部分，确认每个返回参数的名称、数据类型、是否为必需以及任何相关的备注信息。调用接口并分析返回的数据，验证返回参数是否符合文档描述。

11.4 接口使用证实

11.4.1 检查平台的 API 文档或用户手册，确认其中是否详细描述了企业注册的接口调用流程、是否存在用于上传材料的接口。

11.4.2 与平台运营方沟通或查阅相关文档，了解审核流程的具体步骤和标准。观察或记录一个真实的审核过程，确认其是否符合既定的流程和标准。

11.4.3 在审核通过后，检查平台是否自动生成了认证信息（如 API 密钥、访问令牌等），并将其提供给使用方。验证这些认证信息是否能够正常使用，并且是否具有适当的权限控制。

11.4.4 审查平台的隐私政策和服务协议，确认其中是否明确规定了对用户信息的保密义务。进行安全测试，尝试通过各种手段获取使用方的信息，验证平台是否有有效的安全措施防止信息泄露。

11.5 接口安全证实

11.5.1 查阅 API 文档和相关的安全策略文档。

11.5.2 使用专业的安全测试工具和方法，对平台进行渗透测试、漏洞扫描等。

11.5.3 由第三方安全机构对平台进行全面的合规性评估。

11.5.4 应部署安全信息和事件管理系统，实时监控平台的安全状态。