



工业互联网产业联盟标准

AII/007-2022

工业互联网标识解析 接入认证系统接口 技术要求

Identification and Resolution System for the
Industrial Internet—Technical requirements for
interface of access authentication system

工业互联网产业联盟

(2022年5月16日发布)

目 次

| | |
|------------------------|----|
| 前 言 | II |
| 1 范围 | 3 |
| 2 规范性引用文件 | 3 |
| 3 术语和定义 | 3 |
| 4 概述 | 3 |
| 5 功能要求 | 3 |
| 5.1 数据同步 | 3 |
| 5.2 接入认证 | 4 |
| 6 接口要求 | 4 |
| 6.1 数据同步接口 | 4 |
| 6.1.1 新增节点数字证书接口 | 4 |
| 6.1.2 更新节点数字证书接口 | 5 |
| 6.1.3 删除节点数字证书接口 | 5 |
| 6.2 接入认证接口 | 5 |
| 7 接口异常返回值 | 6 |
| 8 数据同步节点信息 | 6 |

前 言

本文件为工业互联网标识解析安全系列标准之一。
随着技术的发展，还将制定后续的相关标准。

本文件起草单位：恒安嘉新（北京）科技股份公司、中国信息通信研究院、北京数字认证股份有限公司、北京安信天行科技有限公司、北京科技大学、郑州信大捷安信息技术股份有限公司、北京启明星辰信息安全技术有限公司。

本文件主要起草人：许道远、刘阳、马宝罗、古定健、田娟、池程、李蓉、王泽政、张振涛、李鹏超、孔令毫、谢滨、李述胜、樊新海、陈红松、翟建军、刘献伦、刘为华、赵军凯。



工业互联网产业联盟
Alliance of Industrial Internet

工业互联网标识解析 接入认证系统接口技术要求

1 范围

本文件规定了工业互联网标识解析体系中的国家顶级节点、二级节点、企业节点和公共递归节点提供接入认证系统接口相关的功能要求、接口要求、接口异常返回值、数据同步节点信息。

本文件适用于工业互联网标识解析接入认证系统接入认证接口开发，以及与国家顶级节点、二级节点、企业节点和公共递归节点对接使用。

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；不注日期的应用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 33745-2017 物联网术语

GB/T 35285-2017 信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业互联网 industrial internet

工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施。

3.2

标识解析 Identifier resolution

将标识符翻译成与其相关联的信息的过程。

[来源：GB/T 33745-2017，定义2.4.3]

4 概述

工业互联网标识解析接入认证系统是基于国密算法为核心支撑的公钥认证机制为国家顶级节点、二级节点、企业节点、公共递归解析节点提供整体安全认证服务的系统。工业互联网标识解析接入认证系统接口对外提供数据同步接口和接入认证接口两部分。工业互联网标识解析接入认证系统数据同步接口是面向国家顶级节点、二级节点、企业节点提供节点数字证书信息同步服务，同时接入认证接口是面向工业互联网标识解析体系中的国家顶级节点、二级节点、企业节点和公共递归节点提供节点间的安全身份认证。

5 功能要求

5.1 数据同步

工业互联网标识解析接入认证系统为各个节点提供认证数据同步服务接口，根据指定同步请求条件，返回数据同步接口结果信息。数据同步请求数据格式和数据同步结果返回数据格式见第6.1节。详细流程见《工业互联网标识解析接入认证技术要求》第5节数字证书申请业务流程。如图1所示。

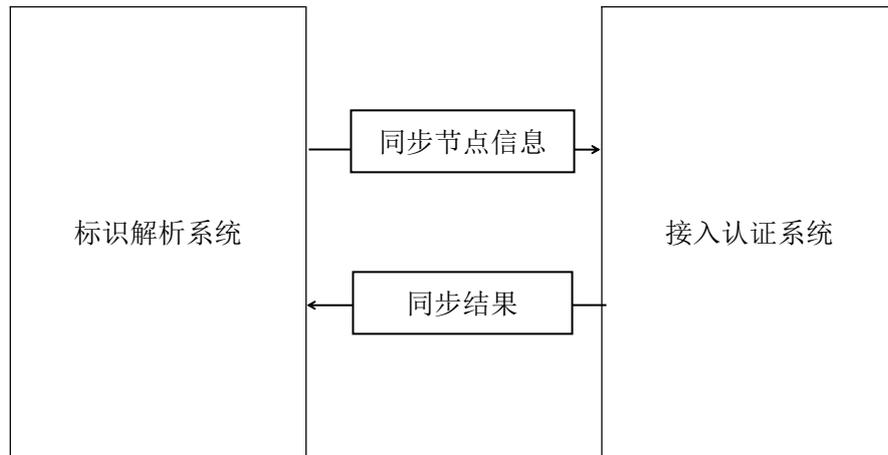


图 1 数据同步接口

5.2 接入认证

工业互联网标识解析接入认证系统为各个节点提供统一接入认证接口，根据指定查询条件，返回核查结果信息。接入认证请求数据格式和接入认证结果返回数据格式见 第6.2节。详细流程见《工业互联网标识解析接入认证技术要求》第5节节点接入认证流程。如图2所示。

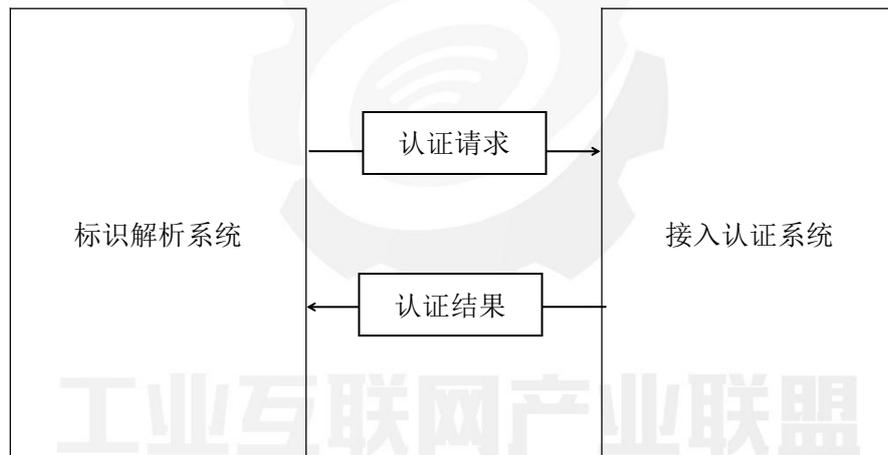


图 2 接入认证接口

6 接口要求

6.1 数据同步接口

6.1.1 新增节点数字证书接口

接口名称：Createnode，同步新增节点的信息，根据节点信息制作节点数字证书。

参数说明：见表1

表 1 新增节点数字证书方法参数说明

| 参数名称 | 参数类型 | 描述 |
|---------------|---------------|-------------|
| nodeInfoParam | NodeInfoParam | 节点信息，见第 8 节 |

返回值说明：字符串，当status为0时表示新增成功，其他信息新增失败；当message为0时表示新增成功，其他信息为错误信息；当cert为2000时标识数字证书新增失败，其他为证书具体信息（base64格式）。

6.1.2 更新节点数字证书接口

接口名称: Updatenode, 同步节点的更新信息, 根据更新节点信息制作节点数字证书。

参数说明: 见表2

表 2 更新节点数字证书方法参数说明

| 参数名称 | 参数类型 | 描述 |
|---------------|---------------|-------------|
| nodeInfoParam | NodeInfoParam | 节点信息, 见 8 节 |

返回值说明: 字符串, 当status为0时表示更新成功, 其他信息更新失败; 当message为0时表示修改成功, 其他信息为错误信息; 当cert为2000时String标识数字证书更新失败, 其他为证书具体信息(base64格式)。

6.1.3 删除节点数字证书接口

deletenode, 同步节点的删除消息, 根据节点删除消息吊销节点数字证书的方法。

参数说明: 见表3

表 3 删除节点数字证书方法参数说明

| 参数名称 | 参数类型 | 描述 |
|--------|--------|----------------|
| openId | String | 唯一标识, 最长 32 字符 |

返回值说明: 字符串, 当status为0时表示删除成功, 其他信息删除失败; 当message为0时表示删除成功, 其他信息为错误信息。

6.2 接入认证接口

接口名称: Authentication, 根据公钥证书、待证书签名数据原文、随机数、时间戳等数据生成登录签名值。

参数说明: 见表4

表 4 登录签名方法参数说明

| 参数名称 | 参数类型 | 描述 |
|----------|--------|-----------------|
| userCert | String | 公钥证书(base64 格式) |
| signData | byte[] | 待证书签名数据原文 |
| random | String | 随机数(10 位) |
| time | String | 时间戳 |

返回值说明: 字节数组, 为2000时表示登录签名失败, 其他为签名值(返回pkcs1格式的签名值的base64 编码)。

接口名称: authenticationVerifySignedData, 根据签名证书、待验证的数据原文、签名值等数据验证登录签名值。

参数说明: 见表5

表 5 登录验证方法参数说明

| 参数名称 | 参数类型 | 描述 |
|----------|--------|-----------------|
| userCert | String | 签名证书(base64 格式) |

| | | |
|-----------|--------|----------|
| signData | byte[] | 待验证的数据原文 |
| signValue | byte[] | 签名值 |

返回值说明：字符串，为2000时表示验证失败，其他为认证令牌token。

接口名称：getSignedNodeData，根据令牌获取节点信息的方法。

参数说明：见表6

表 6 获取节点信息方法参数说明

| 参数名称 | 参数类型 | 描述 |
|-------|--------|----|
| token | String | 令牌 |

返回值说明：字符串，为2000时表示获取失败，其他为节点信息nodeInfoParam。

7 接口异常返回值

接口异常返回值说明见表7。

表 7 接口异常返回值

| 错误码 | 描述 |
|--------|----------------|
| 000000 | 系统错误 |
| 000002 | 请求中必须包含必要标识 |
| 000004 | 无操作权限 |
| 000005 | 参数非法（具体非法参数信息） |

8 数据同步节点信息

数据同步节点信息说明见表8。

表 8 数据同步节点 nodeinfo 信息

| 参数名称 | 参数类型 | 描述 | 是否必填 |
|---------------------|--------|---|------|
| nodeType | String | 节点类型： 1-国家顶级节点 2-二级节点 3-企业节点 4-公共节点 | 是 |
| nodeName | String | 节点名称 | 是 |
| area | String | 组织/单位注册所在地域 | 是 |
| businesslicense | image | 组织/单位营业执照 | 是 |
| Ip | String | 节点 ip 地址 | 是 |
| prefix | String | 前缀 | 是 |
| channelName | String | 渠道名称 | 是 |
| appSubordinateUnits | String | 应用归属单位 | 是 |
| appName | String | 应用系统名称 | 是 |
| unitName | String | 单位名称 | 是 |
| unitPhone | String | 单位电话 | 否 |

| | | | |
|-------------------------|--------|----------|---|
| Address | String | 通信地址 | 否 |
| authorizedRepresent | String | 法定代表人 | 是 |
| authorizedPhone | String | 法人手机号 | 是 |
| certificateType | String | 法人证件类型 | 是 |
| certificateCode | String | 法人证件号 | 是 |
| operatorName | String | 经办人姓名 | 否 |
| operatorPhone | String | 经办人手机号 | 否 |
| operatorEmail | String | 经办人邮箱 | 否 |
| operatorCertificateType | String | 经办人证件类型 | 否 |
| operatorCertificateCode | String | 经办人证件号 | 否 |
| certificateForUSCC | String | 统一社会信用代码 | 是 |
| otherCertificateType | String | 其他证件类型 | 否 |
| otherCertificateCode | String | 其他证件号码 | 否 |



工业互联网产业联盟
Alliance of Industrial Internet