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

工 业 互 联 网 产 业 联 盟 标 准

AII/006-2022

工业互联网标识解析 接入认证技术要求

Identification and Resolution System for the Industrial Internet- Technical requirements for access authentication

工业互联网产业联盟

（2022 年 5 月 16 日发布）

目　　次

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：中国信息通信研究院、恒安嘉新（北京）科技股份公司、北京数字认证股份有限公司、北京科技大学、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：马宝罗、刘阳、田娟、池程、许道远、古定建、谢滨、陈红松、刘为华、刘献伦。

工业互联网标识解析 接入认证技术要求

1 范围

本文件规定了工业互联网标识解析节点接入时的数字证书申请、认证业务流程及管理要求、接入认证功能要求。

本文件适用于工业互联网标识解析接入认证体系的建设、管理等。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 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

GB/T 32918.2-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法

GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范

YD/T 2127.1-2010 移动 Web 服务网络身份认证技术要求 第 1 部分：总体技术要求

GB/T 38637.1-2020 物联网 感知控制设备接入 第 1 部分 总体要求

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

根据标识编码查询目标对象网络位置或者相关信息的系统装置。

[来源：GB/T 33745-2017，定义2.4.3]

4 缩略语

下列缩略语适用于本文件。

CA：证书颁发机构（Certificate Authority）

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer）

IP：互联网协议（Internet Protocol）

OCSP：在线证书状态协议(Online Certificate Status Protocol)

RA：注册机构（Registration Authority）

5 概述

工业互联网标识解析接入认证体系是面向国家顶级节点、二级节点、企业节点、递归解析节点提供基于国密算法的公钥认证安全服务体系，包括身份认证服务和数据安全传输服务。标识解析接入认证能力应具备身份管理功能、数字证书管理功能和身份认证功能。工业互联网标识解析接入认证体系有两类角色：

a) 被认证主体方：国家顶级节点、二级节点、企业节点和递归解析节点；

b) 认证服务提供方：CA 中心、接入认证系统。CA 中心亦可包含在接入认证系统。

6 数字证书申请

6.1 数字证书申请流程

工业互联网标识解析各级节点在接入体系时，需首先申请数字证书，其中二级节点和企业节点的证书申请可与标识注册同步进行。数字证书申请业务流程见图 1。

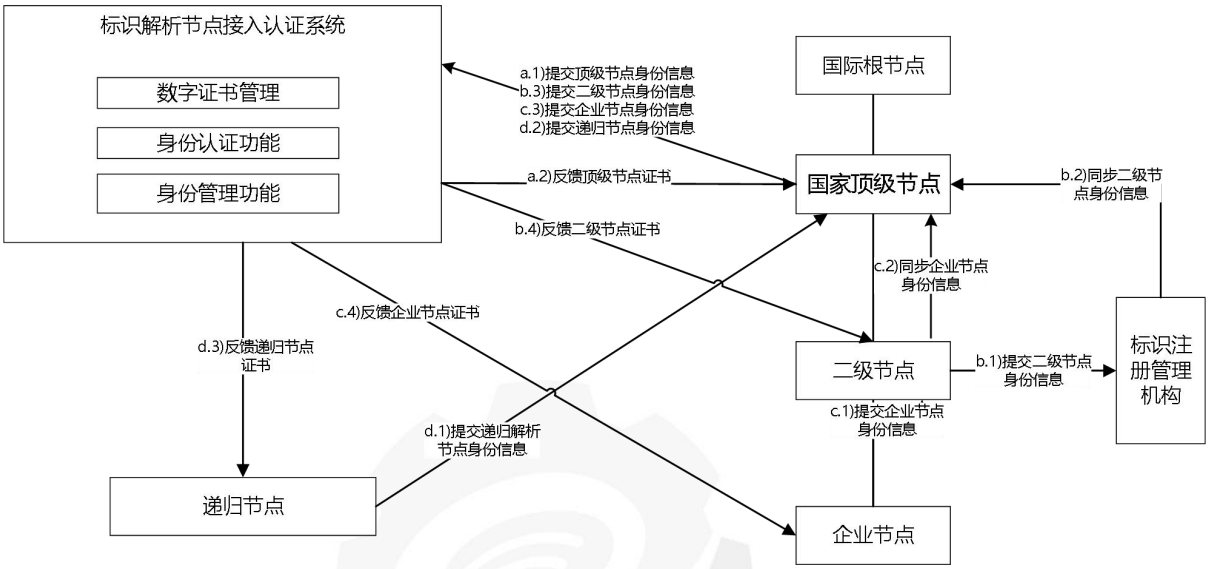

图 1 数字证书申请业务流程

6.2 国家顶级节点申请流程

a.1）国家顶级节点向标识解析节点接入认证系统提交数字证书申请请求，证书申请信息见表 1；
a.2）CA 中心为国家顶级节点签发数字证书，CA 中心使用自己的私钥对用户身份和用户公钥进行绑定，生成数字证书分发给国家顶级节点。

表 1 证书申请信息

字段号	字段名称		填写说明
01	证书业务类型		以下选项选择其一填写： ☐初次办理 ☐证书更新 ☐信息变更 ☐丢失/损坏补办 ☐密码解锁 ☐证书吊销 ☐证书退货
02	证书有效期		/
03	证书应用信息	渠道名称	/
		应用归属单位	/
		应用系统名称	/
04	申请单位信息	单位名称	/
		单位电话	/
		通信地址	/

05	法人信息	法定代表人	/
		法人手机号	/
		法人证件类型	/
		法人证件号	/
06	经办人信息	经办人姓名	/
		经办人手机号	/
		经办人邮箱	/
		经办人证件类型	/
		经办人证件号	/
07	企业基本信息	统一社会信用代码	/
		其他证件类型	/
		其他证件号码	/

6.3 二级节点申请流程

b.1）二级节点向标识注册管理机构提交二级节点身份信息（含证书申请信息），证书申请信息见表 1；

b.2）标识注册管理机构将二级节点身份信息同步给国家顶级节点；

b.3）国家顶级节点将二级节点身份信息发送给标识解析接入认证系统；

b.4） CA 中心为二级节点签发数字证书，CA 中心使用自己的私钥对用户身份和用户的公钥进行绑定，生成数字证书分发给二级节点。

6.4 企业节点申请流程

c.1）企业节点向二级节点服务机构提交企业节点身份信息（含证书申请信息），证书申请信息见表 1；

c.2）二级节点将企业节点身份信息同步给国家顶级节点审核；

c.3）国家顶级节点将将企业节点身份信息发送给标识解析接入认证系统；

c.4） CA 中心为企业节点签发数字证书，CA 中心使用自己的私钥对用户身份和用户的公钥进行绑定，生成数字证书分发给企业节点。

6.5 递归节点申请流程

d.1）递归节点向国家顶级节点提交递归解析节点身份信息（含证书申请信息），证书申请信息见表 1；

d.2）国家顶级节点将递归节点身份信息发送给标识解析接入认证系统；

d.3）认证机构 CA 为递归节点签发数字证书，CA 使用自己的私钥对用户身份和用户的公钥进行绑定，生成数字证书分发给递归节点。

6.6 数字证书更新机制

递归节点生成认证请求过程中，若发现节点数字证书已过期，转到数字证书管理模块进行数字证书更新后生成认证请求；顶级节点、二级节点、企业节点在生成签名信息时，若发现节点数字证书已过期，转到数字证书管理模块进行数字证书更新后生成签名信息。

7 标识解析节点接入认证流程及管理要求

当客户端发起解析请求时，节点在提供解析服务时应同步对节点身份进行双向认证。认证步骤如下：

a) 客户端向递归节点发送标识解析请求；
b) 递归节点在本地缓存中未查到该请求的标识信息，递归节点将请求消息签名后发送给国家顶级节点；
c) 国家顶级节点对签名的请求信息进行验签，核验递归节点的真实性和消息的完整性，核验通过后将二级节点解析记录信息签名后反馈递归节点；
d) 递归节点对签名信息进行验证，核验国家顶级节点的真实性和二级节点解析记录信息的完整性。核验通过后将签名后的请求消息发送二级节点；
e) 二级节点签名的请求信息进行验签，核验递归节点的真实性和解析请求消息的完整性，核验通过后将企业节点解析记录信息签名后反馈给递归节点；
f) 递归节点对签名进行验证，核验企业节点的真实性和解析记录信息的完整性，核验通过后将签名后的解析请求消息发送企业节点；
g) 企业节点核验递归节点的真实性和请求消息的完整性，核验通过后将解析结果签名后反馈给递归节点；
h) 递归节点进行验签，核验企业节点的真实性和解析结果的完整性和真实有效性，将解析结果进行缓存，同时将解析结果反馈给标识解析请求客户端。

工业互联网标识解析节点接入认证业务流程见图 2。

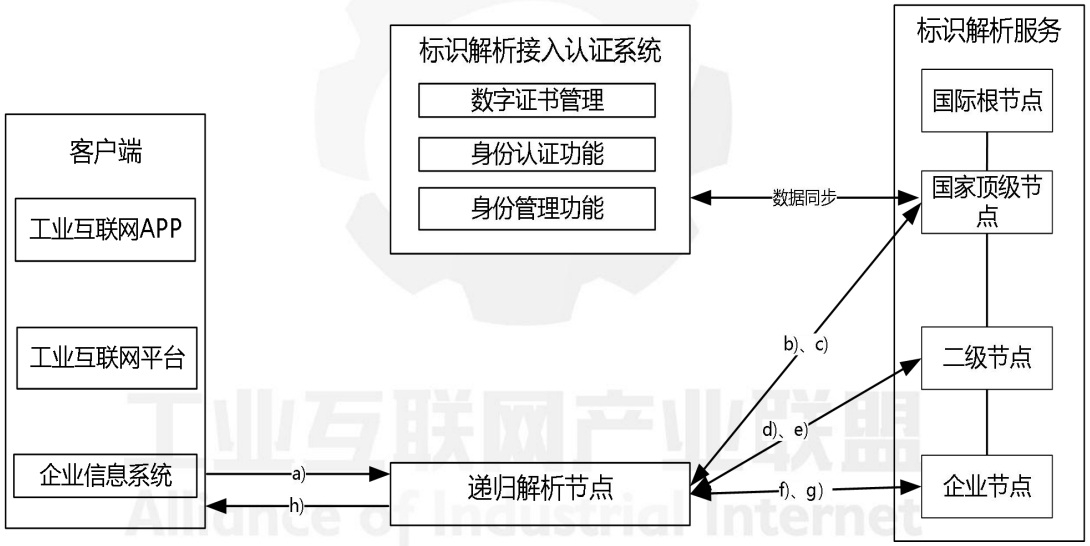

图 2　工业互联网标识解析节点接入认证业务流程

当递归节点有解析缓存时，递归节点直接将解析结果反馈给标识解析请求客户端。

8　标识解析节点接入认证功能要求

8.1　数字证书管理

负责数字证书的签发、管理、撤销、查询等证书管理，以及相应的密钥管理工作。具备 CA 签发、CA 管理、RA 注册管理、OCSP 证书状态查询、证书审计管理等服务功能。为保证系统的安全可控，默认采用国产的密码算法，当需要与国际根节点下的标识解析体系进行认证时，采用通用算法。

8.2　身份认证功能

身份认证功能指面向标识解析各级节点提供给统一的身份认证服务。身份认证功能应具备节点认证、安全登录、自助服务等功能。

8.3 身份管理功能

向国家顶级节点、二级节点、递归节点、企业节点、标识解析客户端提供授权管理、访问控制、身份信息同步、审计管理、凭证管理等服务的能力。