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/004-2023

工业互联网标识解析 可信解析

Identification and resolution system for the Industrial Internet - Trusted resolution

工业互联网产业联盟

（2023 年 9 月发布）

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。

本文件起草单位：中国信息通信研究院、北京航空航天大学、北京科技大学、奇安信科技集团股份有限公司、郑州信大捷安信息技术股份有限公司、浪潮云洲工业互联网股份有限公司、北京数字认证股份有限公司、启明星辰信息技术集团股份有限公司、恒安嘉新（北京）科技股份公司、中国电信股份有限公司研究院、亚信科技（成都）有限公司

本文件主要起草人：马宝罗、池程、刘阳、田娟、关振宇、陈红松、谢滨、王健楠、刘献伦、李波、古定健、杨震、尹子航、赵军凯、许道远、吴天飞

T11/004 2023

工业互联网标识解析 可信解析

1 范围

本文件规定了工业互联网标识解析体系在提供可信解析服务方面的要求，包括标识解析身份可信、内容可信、行为可信、运营可信要求。

本文件适用于安全可信的工业互联网标识解析体系设计、开发部署和管理。

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

AII/006-2022 工业互联网标识解析 接入认证技术要求

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 identification

工业互联网标识是指在一定范围内唯一地识别工业涉及的物理对象（机器设备、物料、产品等）和信息对象（逻辑实体、资源、服务、文件、数据等）的一种属性。基于该标识，工业互联网和应用能够对目标对象进行控制和管理，以及相关信息的获取、处理、传送与交换等操作。

3.3

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

构建安全可信的工业互联网标识解析体系，满足身份可信、内容可信、行为可信、运营可信等方面的具体要求。

身份可信要求，包括标识注册备案信息、标识解析节点身份；

内容可信要求，包括标识解析数据加密、传输安全、数据同步和备份；

行为可信要求，包括访问控制、账户权限控制、应用资源控制；

运营可信要求，包括对标识解析系统安全、运营管理、物理环境管理。

5 身份可信要求

5.1 标识注册备案要求

5.1.1 标识注册者实名制审核需提供的资料及信息

标识注册者应出示相关资料原件并收集标识编码注册者身份证明资料，包括：营业执照正副本复印件或扫描件，工商行政管理局出具的企业证明资料复印件或扫描件，以及组织机构联系人身份证明文件、移动电话、固定电话、电子邮箱。

5.1.2 标识编码注册实名核验的内容

申请单位信息、法人信息、经办人信息、企业基本信息等信息的真实性和合规性核验。

5.1.3 标识编码注册实名核验的方式

注册者通过申请机构向备案机构提交指定的资料和信息，由备案机构对用户的标识编码和身份进行审查，并对标识编码的注册结果产生影响。

5.2 标识解析节点可信要求

5.2.1 公钥的发布方式

标识解析体系中的权威服务通过数字证书发布本区的公钥。公钥记录通常应包含如下内容：

a) 公钥记录作为标识解析系统中的一条资源记录，应当归属于某个标识；

b) 应采用国密算法，如SM2；

5.2.2 信任链的构成

为验证下级公钥记录的真实性，需要将公钥的摘要提交给上级标识解析服务。

摘要记录通常应包含如下内容：

a) 给出生成摘要记录时使用的摘要算法，为算法分配算法号或算法名。在制定通信协议时，使用标准的算法号或算法名，见表1。

表 1 摘要算法

算法号	算法名	算法描述
01	SHA-1	生成 160bit 的摘要
02	SHA-256	生成 256bit 的摘要

b) 按照指定的摘要算法，计算公钥记录的摘要。其中公钥记录的字段至少应包括公钥记录的标识、算法、公钥、其他自定义内容。

c) 摘要记录对应的公钥记录，按照特定算法计算出的标签值。

6 摘要记录对应的公钥记录使用的算法，应当与公钥记录中的对应字段相同。内容可信要求

6.1 数据传输要求

包括采用加解密、数字签名等等技术，确保数据传输安全。

a）解析系统之间的数据交互需要基于安全链接 SSL；

b）应采用内外网隔离或加密等保护措施避免远程访问时数据在公共互联网的明文传输；

c）采用密码技术、数据脱敏、校验技术、数字签名等技术，保证传输数据的保密性、完整性、可用性；

d）在数据迁移前对数据进行本地备份和网络安全能力评估，保证数据迁移不影响业务应用的连续性；

e）在数据迁移、上云、跨境等传输过程中，开展数据安全监测。

6.2 数据存储安全

包括基于密码技术、分类分级管理、存储介质安全管控等手段，保障数据存储安全。

a）根据存储数据量、数据重要性、敏感程度等因素，选择合适的存储介质，做好数据存储介质安全管控或数据碎片化存储；

b）应在保证密码算法安全性的前提下为用户提供对密码算法、强度和方式等参数进行配置的功能；

c）应能够检测到数据在存储过程中保密性、完整性、可用性受到破坏，防止数据被泄露、篡改、删除、插入等操作。在数据保密性、完整性、可用性遭到破坏时，应提供授权用户可察觉的告警信息；

d）实施分类分级存储，对确需加密的数据可采用加密技术、数字签名、校验技术等方式，实现存储数据的保密性、完整性和可用性。

6.3 数据处理安全

包括授权、验证，及数据过程保护和回退。

a）应对数据的处理使用进行授权和验证；

b）建立数据导入导出过程保护和回退机制，保障导入导出过程中发生问题时能有效还原和恢复数据。

6.4 数据共享安全

包括数据共享前风险评估、数据加密、数据同步等要求。

a）在数据交换共享前对数据进行风险评估，并根据风险评估情况采取相应防护措施，确保数据交换共享安全合规；

b）可以采用推送数据或者拉取数据等多种策略；

c）交换数据时，同步数据应被加密传输；

d）同步服务器之间需要按设定时间进行数据同步；

e）定时同步可以采用增量方式，支持局部数据动态共享更新，当某一次增量同步失败时，下次增量同步需要同时更新失败数据；

f）同步服务器之间的时间应当同步，建议采用NTP协议或其他技术。

6.5 数据备份要求

包括备份机制建设、重要数据备份和恢复管理、备份失效处置等要求。

a）系统关键设备、重要线路应采用冗余的保护方式，提供数据本地灾难备份与恢复功能；

b）建立对关键数据和重要信息进行备份和恢复的管理和控制机制；

c）根据备份的管理机制，应当定期对系统记录数据相关信息进行备份；

d）在主服务器故障情况下，可启动热备份系统，保证注册、解析等全套标识解析业务的正常运行，保证相关数据和信息及时恢复的能力；

e）当热备份也失效时，能自动或手工启动冷备份系统，通过冷备份系统提供应急服务。

7 行为可信要求

7.1 访问控制

设定访问控制规则，根据设定的安全策略控制用户到服务器查询时对系统程序、文件、数据库表等资源的访问，访问控制的覆盖范围需要包括与系统资源访问相关的主体、客体及它们之间的各种操作。

a）应提供访问控制功能，对使用应用程序的用户分配账户及相应的访问操作权限；

b）提供明确的允许/拒绝访问控制，能对某具体 IP 地址或 IP 网段进行控制，并防止地址欺骗。

c）应重命名或删除默认账户，修改默认账户的默认登录口令；

d）应及时删除或停用多余的、过期的账户，避免共享账户的存在；

e）应避免将业务服务器直接连接外部系统或网络，系统内各功能区域间采取可靠的技术隔离手段；

f）服务器所在的局域网应该有包过滤机制，以阻断来自服务端口以外的端口访问。

7.2 账户权限控制

包括设备安装原则、漏洞评估、数据库权限设置和等级划分等要求。

a）遵循最小安装的原则，仅为设备安装需要的组件和应用程序；

b）关闭设备中不需要的端口与服务；

c）应能及时发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

d）主机应安装主流防病毒软件并具备及时升级能力，应能检测升级软件的真实性和完整性；

e）设置各个账户的访问策略，并严格限制默认系统账户的访问权限；

f）用户密码应有复杂度要求，并定期更换；

g）应及时删除多余的、过期的账户，避免共享账户的存在；

h）应为操作系统和数据库系统特权用户的分配不同的账户，且彼此管理权限分离。

7.3 应用资源控制

包括最大并发量、会话控制、系统资源负载限制等进行要求。

a）应能够对应用的最大并发会话连接数进行限制；

b）应能够对单个用户、终端、IP 地址的多重并发会话进行限制；

c）应能够对用户或进程对终端设备系统资源的最大使用限度进行限制，防止终端设备被提权；

d）实时监控系统资源负载，包括硬盘、内存、CPU、网络带宽等；当超出阈值时，发出告警。

8 运营可信要求

8.1 系统安全

建立安全检测、软件库更新等机制，保障系统安全。

a）应对构建系统结构的计算机、服务器、网络设备等硬件设备进行必要的安全检测，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定；

b） 操作系统应遵循最小安装的原则，仅安装和开通需要的功能组件和应用程序，并通过安全方式确保系统补丁及时得到更新；

c）标识解析软硬件应通过安全审计，避免已发现的漏洞造成的安全威胁；

d）定期监测标识解析软件的版本安全性，并及时进行软件版本的升级，防止系统软件漏洞造成的威胁；

e）通用主机应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

f）应禁止除管理员、或者被授权人员之外的其他人或其他服务器，从标识解析服务器上上传下载数据，并且对每次上传下载数据做日志记录，并对上传下载的数据做杀毒和镜像备份；能够查询每次上传下载记录和导出上传下载数据文件。

8.2 安全审计

针对用户操作安全审计、审计记录、审计范围等提出具体要求。

a）应提供覆盖标识解析体系用户操作安全审计功能，应对重要安全事件进行审计；

b）审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果，解析系统的运行状况、流量、解析标识访问量和用户行为等进行日志记录；

c）审计范围应覆盖到解析系统用户和数据库用户，包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

d）应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

8.3 运营管理要求

包括对安全管理制度、安全管理人员、安全建设管理、安全开发管理、安全运维管理提出安全防护要求。

a）安全管理制度：包括安全策略及其制定、发布、评审和修订等；

b）安全管理人员：包括岗位设置、人员配备、授权和审批、人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等；

c）安全建设管理：包括安全方案设计、产品采购和使用、工程实施、测试验收、系统交付、服务供应商选择等；

d）安全开发管理：包括安全开发设计、代码审计等；

e）安全运维管理：包括环境管理、介质管理、安全审计、恶意代码防范、设备维护管理、安全事件处置等。

8.4 物理环境要求

包括对物理位置选取、访问控制、防火防潮、供电线路、通信线缆等物理环境提出安全要求。

a）机房场地应选择在具有防震、防风和防雨等能力的建筑内， 避免设在建筑物的顶层或地下室；

b）机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；

c）应将设备或主要部件进行固定，并设置明显的不易除去的标记；

d）应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；

e）应将各类机柜、设施和设备等通过接地系统安全接地；

f）机房应设置灭火设备，设置火灾自动消防系统；

g）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

h）应安装防静电地板并采用必要的接地防静电措施；

i）应在机房供电线路上配置稳压器和过电压防护设备；

j）电源线和通信线缆应隔离铺设，避免互相干扰。