



工业互联网产业联盟标准

AII/017-2021

工业互联网标识解析 主动标识载体 总体技术框架

Industrial Internet Identification and
Resolution—Active Identifier Carrier—General
Technical Framework

工业互联网产业联盟

(2021 年 12 月 30 日发布)

目 次

前 言.....	III
1 范围.....	4
2 规范性引用文件.....	4
3 术语和定义.....	4
3.1.....	4
3.2.....	4
3.3.....	4
3.4.....	4
3.5.....	4
3.6.....	4
3.7.....	4
4 缩略语.....	5
5 主动标识载体分类.....	5
6 总体技术架构和能力.....	5
6.1 总体技术架构.....	5
6.2 主动标识载体能力.....	6
6.3 工业终端能力.....	6
6.4 主动标识载体管理模块能力.....	7
6.5 主动标识载体安全认证服务平台能力.....	7
6.6 数据采集模块能力.....	7
6.7 企业节点基本功能模块能力.....	7
6.8 二级节点能力.....	7
6.9 顶级节点能力.....	7
7 接口技术要求.....	8
7.1 顶级节点企业 CA 管理接口.....	8
7.2 主动标识载体管理接口.....	8
7.3 主动标识载体业务接口.....	8
8 模块之间的基本业务流程.....	9
8.1 基本业务流程综述.....	9
8.2 主动标识载体获得身份凭证 C1.....	9
8.3 主动标识载体管理模块通过主动标识载体安全认证服务平台向主动标识载体写入工业互联网标识.....	11
8.4 主动标识载体管理模块通过主动标识载体安全认证服务平台从主动标识载体读取工业互联网标识.....	13
8.5 主动标识载体管理模块通过主动标识载体安全认证服务平台删除主动标识载体中的工业互联网标识.....	14
8.6 主动标识载体管理模块通过主动标识载体安全认证服务平台修改主动标识载体中的工业互联网标识.....	15
8.7 终端工业应用 APP 读取主动标识载体中的工业互联网标识.....	15
8.8 基于主动标识载体的主动数据上报.....	16
附 录 A.....	18
主动标识载体在电梯监控场景中的应用示例.....	18



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

前 言

本文件为工业互联网主动标识载体系列标准之一。
随着技术的发展，还将制定后续的相关文件。

本文件牵头单位：中国联合网络通信集团有限公司

本文件起草单位和主要起草人：

- 中国联合网络通信集团有限公司：贾雪琴、黄蓉、荆雷、史可、林晨、韩政鑫
- 中国信息通信研究院：刘阳、刘澍、田娟、谢滨、尹子航
- 联通华盛通信有限公司：孙阳阳、韩梦梦
- 紫光国芯微电子股份有限公司：霍航宇
- 中移物联网有限公司：柳耀勇、习熹、肖青
- 联通智慧安全科技有限公司：姚韬、蒋小燕
- 中国电信：李洁、刘伟、龚晟
- 联通物联网有限责任公司：曹侃、张律、谢仁芳
- 芯昇科技有限公司：孙东昱 刘勇
- 联通（黑龙江）产业互联网有限公司：吕威，李博鑫，张笑泳
- 华为技术有限公司：郑秀丽、张婷、潘伟、杨言
- 中兴通讯股份有限公司：游世林，高峰，林兆骥
- 信大捷安：刘为华、刘献伦
- 四川长虹智能制造技术有限公司： 郅慧、符欣
- 浙江吉时工业标识解析技术有限公司：俞正林、华路锋、张小聪
- 诺得物流股份有限公司：赵国荣，赵颀，吕斌
- 北京科技大学：王健全、孙雷、李卫
- 联通（江苏）产业互联网有限公司：于谦
- 宜通世纪科技股份有限公司：王永斌
- 合肥达朴汇联科技有限公司 张焱、李汪红

工业互联网标识解析 主动标识载体 总体技术框架

1 范围

本文件规定了主动标识载体的分类、总体技术框架和能力、接口技术要求以及模块之间的基本业务流程。

本文件适用于工业互联网主动标识载体使用方、提供方、管理方等提供载体适用和管理技术参考。

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。

工业互联网联盟标准《工业互联网标识解析 主动标识载体 通用集成电路卡（UICC）技术要求》

工业互联网联盟标准《工业互联网标识解析 主动标识载体 安全芯片技术要求》

工业互联网联盟标准《工业互联网标识解析 主动标识载体 通信模组技术要求》

工业互联网联盟标准《工业互联网标识解析 标识编码规范》

3 术语和定义

3.1

标识编码 Identification code

能够唯一识别机器、产品等物理资源和算法、工序等虚拟资源的身份符号。

3.2

标识载体 Identifier carrier

承载标识编码以及标识编码相关信息的物理实体，支持对标识编码以及标识编码相关信息的操作（如读、写等操作）。

3.3

主动标识载体 active identifier carrier

承载工业互联网标识编码的载体，具备联网通信能力，能够主动与标识解析服务节点或标识数据应用平台建立连接，宜承载必要的证书、算法或密钥。

3.4

标识解析二级节点 Secondary-Level node of identification and resolution

指面向特定行业或者多个行业提供标识服务的公共节点。

3.5

主动标识载体标识 Identifier of active identifier carrier

能在一定范围内唯一标识主动标识载体的标识。主动标识载体标识在赋予后宜无法修改和删除，一般由主动标识载体生产方赋予。

3.6

标识解析企业节点 Enterprise node of identification and resolution

面向企业内部提供标识编码注册和标识解析服务的标识服务节点，并通过接入标识解析二级节点对外提供解析服务。

3.7

消息认证码 Message authentication code

是经过特定算法后产生的一小段信息，用于检查某段消息的完整性，以及作身份验证。它可以用来检查在消息传递过程中，其内容是否被更改过，同时可以作为消息来源的身份验证，确认消息的来源。

4 缩略语

下列缩略语适用于本文件。

APP	应用程序	Aplication
CA	证书颁发机构	Certification Authority
HSM	硬件安全模块	Hardware Security Module
IP	网际互联网协议	Internet Protocol
SDK	软件开发工具包	Software Development Kit
UICC	通用集成电路卡	Universal Integrated Circuit Card
URL	统一资源定位符	Uniform Resource Location

5 主动标识载体分类

主动标识载体包括但不限于以下三类：

(1) 通用集成电路卡（UICC）：承载工业互联网标识编码，支持多种加密算法，具安全存储、数据加密/解密、身份认证等功能的通用集成电路卡。具体技术能力参见《工业互联网标识解析 主动标识载体 通用集成电路卡（UICC）技术要求》。

(2) 安全芯片：承载工业互联网标识编码，具备独立安全内核、专用密码算法硬件计算单元、独立安全存储空间，具有地址加扰、加密存储、访问控制功能，支持硬件真随机数，能够抗实验室级软件及物理攻击。具体技术能力参见《工业互联网标识解析 主动标识载体 安全芯片技术要求》。

(3) 通信模组：承载工业互联网标识编码，集成控制器、通信芯片、存储器、支持国密的硬件安全模块等模块，提供标准接口功能，具备主动建立通信连接能力。具体技术能力参见《工业互联网标识解析 主动标识载体 通信模组技术要求》。

主动标识载体通信模组需要具备安全承载工业互联网标识及其相应凭证、支持合法接入主动标识载体服务平台、支持主动标识载体服务平台的标识管理、支持主动标识载体服务平台的凭证管理、支持广域通信网络连接、满足应用场景的业务需求等功能。

6 总体技术架构和能力

6.1 总体技术架构

主动标识载体中存储的工业互联网标识，其编码规则应遵循《工业互联网标识解析 标识编码规范》。主动标识载体总体技术架构见图1所示，涉及终端侧、管理侧和节点侧。

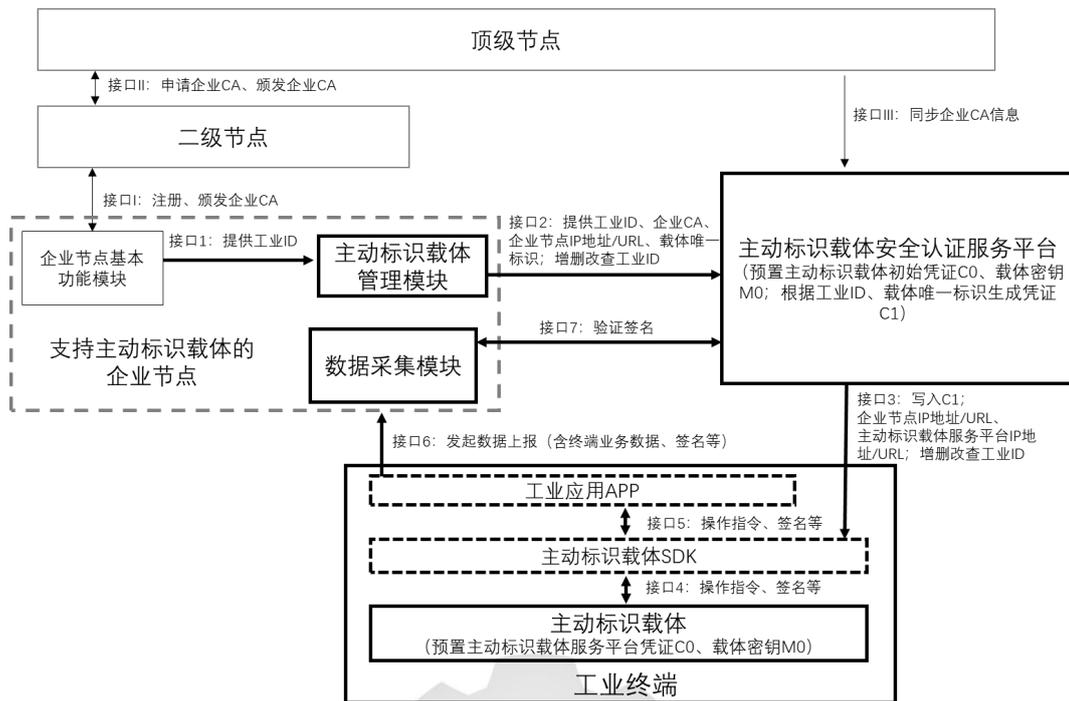


图1 主动标识载体总体技术架构和接口

注：工业ID 是工业互联网标识的简称。

终端侧是指在工业终端部署主动标识载体、主动标识载体SDK及工业应用APP，实现工业互联网标识数据、主动标识载体数据及终端采集数据的上报；管理侧是指主动标识载体安全认证服务平台与工业互联网标识解析体系建立主动标识载体安全认证管理机制，面向工业终端提供主动标识载体的安全认证和载体管理；节点侧是指工业互联网解析体系下顶级节点、二级节点以及支持主动标识载体的企业节点，其中企业节点部署主动标识载体管理模块、数据采集模块，实现主动标识载体管理、工业终端数据采集等操作。

6.2 主动标识载体能力

主动标识载体能力包括但不限于：

- (1) 应支持承载工业互联网标识编码及其必要的身份凭证和安全算法；
- (2) 应支持工业终端主动获取主动标识载体承载的工业互联网标识（无需借助标识读写设备来触发）；
- (3) 应支持根据主动标识载体安全认证服务平台的请求写入、删除、修改、查询、存储工业互联网标识；
- (4) 应支持与主动标识载体安全认证服务平台交互时所需的身份验证流程。

具体类型的主动标识载体技术要求参见《工业互联网标识解析 主动标识载体 通用集成电路卡（UICC）技术要求》、《工业互联网标识解析 主动标识载体 安全芯片技术要求》、《工业互联网标识解析 主动标识载体 通信模组技术要求》。

6.3 工业终端能力

工业终端能力包括但不限于：

- (1) 应支持主动标识载体SDK；
- (2) 应支持主动标识载体安全认证服务平台侧通过主动标识载体SDK与主动标识载体进行互操作（包括终端身份验证等）；

主动标识载体SDK的技术要求参见《工业互联网标识解析 主动标识载体 通用集成电路卡（UICC）技术要求》、《工业互联网标识解析 主动标识载体 安全芯片技术要求》、《工业互联网标识解析 主动标识载体 通信模组技术要求》。

6.4 主动标识载体管理模块能力

主动标识载体管理模块的能力包括但不限于：

- （1）应具备支持从企业节点基本功能模块获取工业互联网标识；
- （2）应具备支持获取主动标识载体标识；
- （3）应具备支持管理主动标识载体标识与工业互联网标识的关联关系；
- （4）应具备支持通过主动标识载体安全认证服务平台对主动标识载体进行工业互联网标识的写入、删除、修改、查询操作。

6.5 主动标识载体安全认证服务平台能力

主动标识载体安全认证服务平台能力包括但不限于：

- （1）应支持根据工业互联网标识、主动标识载体标识等信息生成凭证C1（如数字证书、消息认证码）；
- （2）应通过主动标识载体SDK将工业互联网标识、主动标识载体标识（如手机拨号号码、UICC卡的ICCID、MAC地址等）、企业CA等信息写入到主动标识载体中；
- （3）宜通过主动标识载体SDK将企业节点IP地址或者URL等信息写入到主动标识载体中；
- （4）应能根据主动标识载体管理模块的请求，对主动标识载体中的工业互联网标识进行写入、删除、修改、查询操作；
- （5）应能根据主动标识载体管理模块的请求，响应与工业互联网标识与主动标识载体标识关联关系相关的操作；
- （6）应为主动标识载体分配身份凭证，并应依据身份凭证对主动标识载体的身份进行验证；
- （7）应为数据采集模块提供主动标识载体身份验证结果。

6.6 数据采集模块能力

数据采集模块能力包括但不限于：

- （1）应具备向主动标识载体安全认证服务平台发起对主动标识载体身份验证的能力；
- （1）应具备接收来自终端的业务数据的能力，应具备存储数据的能力；可具备分析数据等能力；

6.7 企业节点基本功能模块能力

与主动标识载体相关的企业节点能力应包括但不限于：

- （1）为主动标识载体分配工业互联网标识；
- （2）通过二级节点向顶级节点申请企业CA；
- （3）与二级节点对接的其他功能。

6.8 二级节点能力

与主动标识载体相关的二级节点能力应包括但不限于：

- （1）为企业节点分配工业互联网标识企业前缀。
- （2）支持企业节点向顶级节点申请企业CA。
- （3）其他技术要求参见《工业互联网标识解析 二级节点技术要求》。

6.9 顶级节点能力

与主动标识载体相关的顶级节点能力应包括但不限于：

- (1) 为二级节点分配工业互联网标识二级节点前缀。
- (2) 通过二级节点向企业节点颁发企业CA证书。
- (3) 其他技术要求参见《工业互联网标识解析 国家顶级节点与二级节点对接技术要求》。

7 接口技术要求

7.1 顶级节点企业 CA 管理接口

顶级节点企业CA管理接口包括：

- (1) 接口I：企业节点基本功能模块与二级节点之间的接口，主要功能应包括但不限于：
 - a. 企业节点应通过二级节点向顶级节点注册、申请企业CA证书；
 - b. 二级节点应向企业节点颁发企业CA证书。
- (2) 接口II：二级节点与顶级节点之间的接口，主要功能应包括但不限于：
 - a. 根据企业节点的请求，二级节点应向顶级节点申请企业CA证书。
 - b. 顶级节点应通过二级节点向企业节点颁发企业CA证书。
- (3) 接口III：顶级节点与主动标识载体安全认证服务平台之间的接口，主要功能包括但不限于：
 - a. 顶级节点应向主动标识载体安全认证服务平台同步企业CA信息。

7.2 主动标识载体管理接口

主动标识载体管理接口包括：

- (1) 接口1：企业节点基本功能模块与主动标识载体管理模块之间的接口，主要功能包括但不限于：
 - a. 企业节点基本功能模块应向主动标识载体管理模块提供工业互联网标识。
- (2) 接口2：主动标识载体管理模块与主动标识载体安全认证服务平台之间的接口，主要功能包括但不限于：
 - a. 主动标识载体管理模块应向主动标识载体安全认证服务平台提供企业CA证书、企业节点IP地址或者URL、主动标识载体标识等；
 - b. 主动标识载体管理模块应通过主动标识载体安全认证服务平台对主动标识载体进行工业互联网标识的写入、删除、修改、查询操作；
 - c. 主动标识载体管理模块应将工业互联网标识、主动标识载体标识、以及工业互联网标识与主动标识载体标识之间的绑定关系同步给主动标识载体安全认证服务平台。
- (3) 接口3：主动标识载体安全认证服务平台与主动标识载体SDK之间的接口，主要功能应包括但不限于：
 - a. 主动标识载体安全认证服务平台应通过主动标识载体SDK向主动标识载体写入凭证C1、企业节点IP地址或者URL、主动标识载体安全认证服务平台IP地址或者URL，并进行工业互联网标识的写入、删除、修改、查询操作。
- (4) 接口4：主动标识载体SDK与主动标识载体之间的接口，主要功能包括但不限于：
 - a. 主动标识载体SDK应将来自主动标识载体安全认证服务平台的凭证C1写入到主动标识载体；
 - b. 主动标识载体SDK应将来自主动标识载体安全认证服务平台的操作指令（包括对工业互联网标识的增删改查操作等）发送给主动标识载体。

7.3 主动标识载体业务接口

主动标识载体业务接口包括：

- (1) 接口5：主动标识载体SDK同工业应用APP之间的接口，主要功能包括但不限于：
 - a. 工业应用 APP 应触发主动标识载体 SDK 读取主动标识载体中的工业互联网标识、主动标识载体标识、身份凭证 C1 等数据；

(2) 接口 4: 主动标识载体 SDK 应通过接口 4 读取主动标识载体中的工业互联网标识、主动标识载体标识、身份凭证 C1 等数据;

(3) 接口 6: 数据采集模块同工业终端工业应用 APP 之间的接口, 主要功能包括但不限于:

a. 工业应用 APP 应向数据采集模块发起数据上报。上报的数据包括但不限于工业互联网标识、主动标识载体标识、终端业务数据、身份凭证 C1 等。

(4) 接口 7: 数据采集模块同主动标识载体安全认证服务平台之间的接口, 主要功能包括但不限于:

a. 数据采集模块应通过主动标识载体安全认证服务平台对主动标识载体的身份进行验证。

8 模块之间的基本业务流程

8.1 基本业务流程综述

图1所示模块之间的基本业务流程包括: 主动标识载体获得身份凭证C1、主动标识载体管理模块通过主动标识载体管理模块向主动标识载体写入工业互联网标识、主动标识载体管理模块通过主动标识载体安全认证服务平台从主动标识载体读取工业互联网标识、主动标识载体管理模块通过主动标识载体安全认证服务平台删除主动标识载体中的工业互联网标识、主动标识载体管理模块通过主动标识载体安全认证服务平台修改主动标识载体中的工业互联网标识、基于主动标识载体的主动数据上报。

8.2 主动标识载体获得身份凭证 C1

8.2.1 前置条件

(1) 主动标识载体

- a. 应生成并存储主动标识载体的密钥M0;
- b. 应在主动标识载体安全认证服务平台注册;
- c. 应预置主动标识载体安全认证服务平台的初始凭证C0。

(2) 主动标识载体安全认证服务平台

- a. 应生成并存储主动标识载体安全认证服务平台的初始凭证C0;
- b. 应预置主动标识载体的密钥M0;
- c. 应获得主动标识载体标识(如UICC卡的ICCID等)、企业CA证书、企业节点IP地址或者URL等信息。

8.2.2 核心流程

主动标识载体向主动标识载体安全认证服务平台申请身份凭证C1的流程见图2。

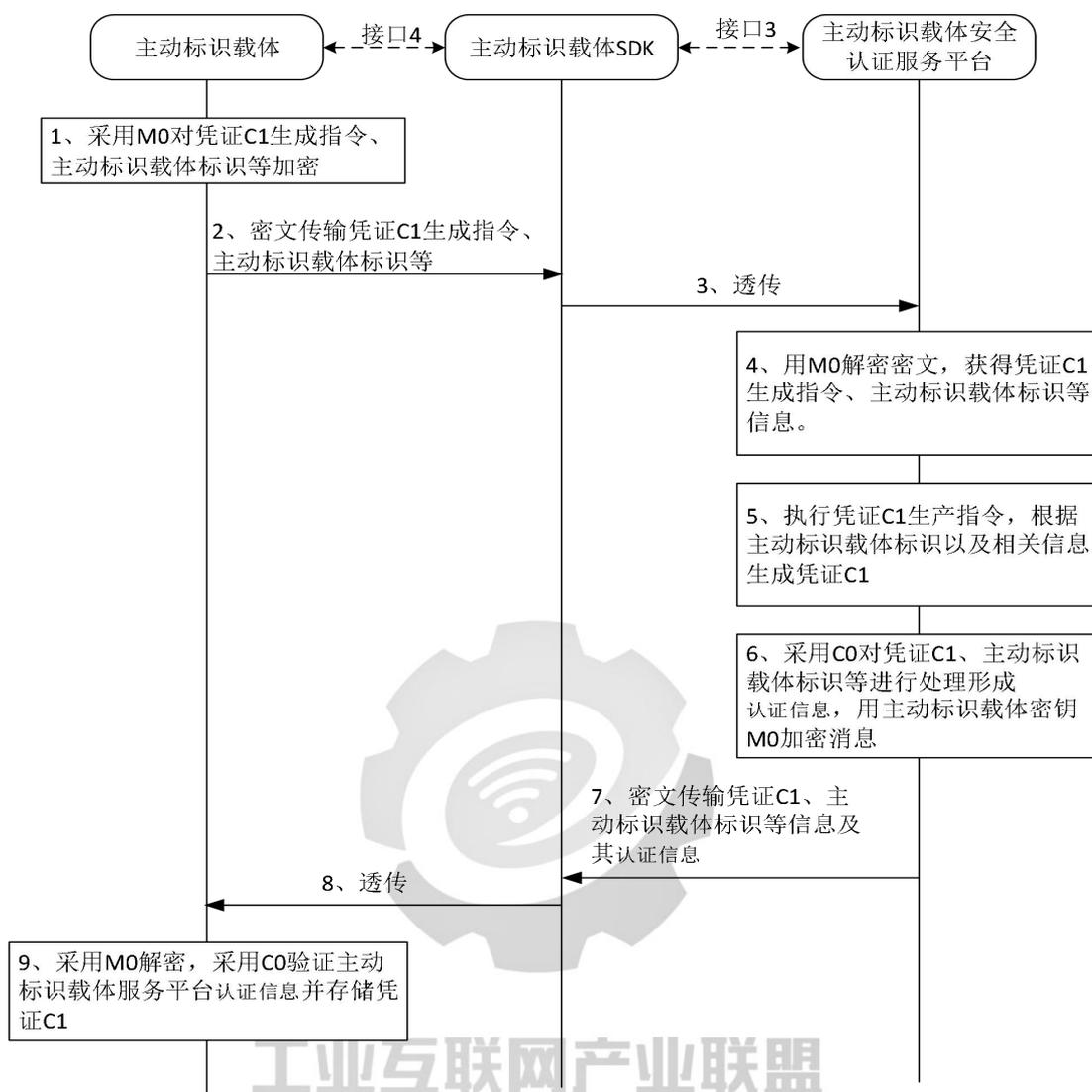


图2 主动标识载体管理模块申请凭证 C1 的流程示例

图2流程说明如下：

- (1) 主动标识载体采用M0对凭证C1生成指令、主动标识载体标识等信息加密，形成密文；
- (2) 主动标识载体将密文发送给主动标识载体SDK；
- (3) 主动标识载体SDK将密文透传给主动标识载体安全认证服务平台；
- (4) 主动标识载体安全认证服务平台采用M0解密密文，获得凭证C1生成指令、主动标识载体标识等信息；
- (5) 主动标识载体安全认证服务平台执行凭证C1生成指令，根据主动标识载体标识以及相关信息生成主动标识载体的凭证C1，如证书或者消息认证码；
- (6) 主动标识载体安全认证服务平台采用C0对凭证C1、主动标识载体标识等进行处理形成认证信息（包括数字签名、消息认证码）；用主动标识载体密钥M0对凭证C1、主动标识载体标识等信息及其认证信息加密，形成密文；
- (7) 主动标识载体安全认证服务平台将密文发给主动标识载体SDK；
- (8) 主动标识载体SDK将密文透传给主动标识载体；

(9) 主动标识载体采用M0解密密文获得凭证C1、主动标识载体标识等信息及其认证信息，采用C0验证认证信息。在认证信息合法的情况下，主动标识载体将凭证C1存储于本地。

8.3 主动标识载体管理模块通过主动标识载体安全认证服务平台向主动标识载体写入工业互联网标识

8.3.1 前置条件

本流程的前置流程见8.2。此外，前置流程还应包括主动标识载体安全认证服务平台获得工业互联网标识的流程，见图3。

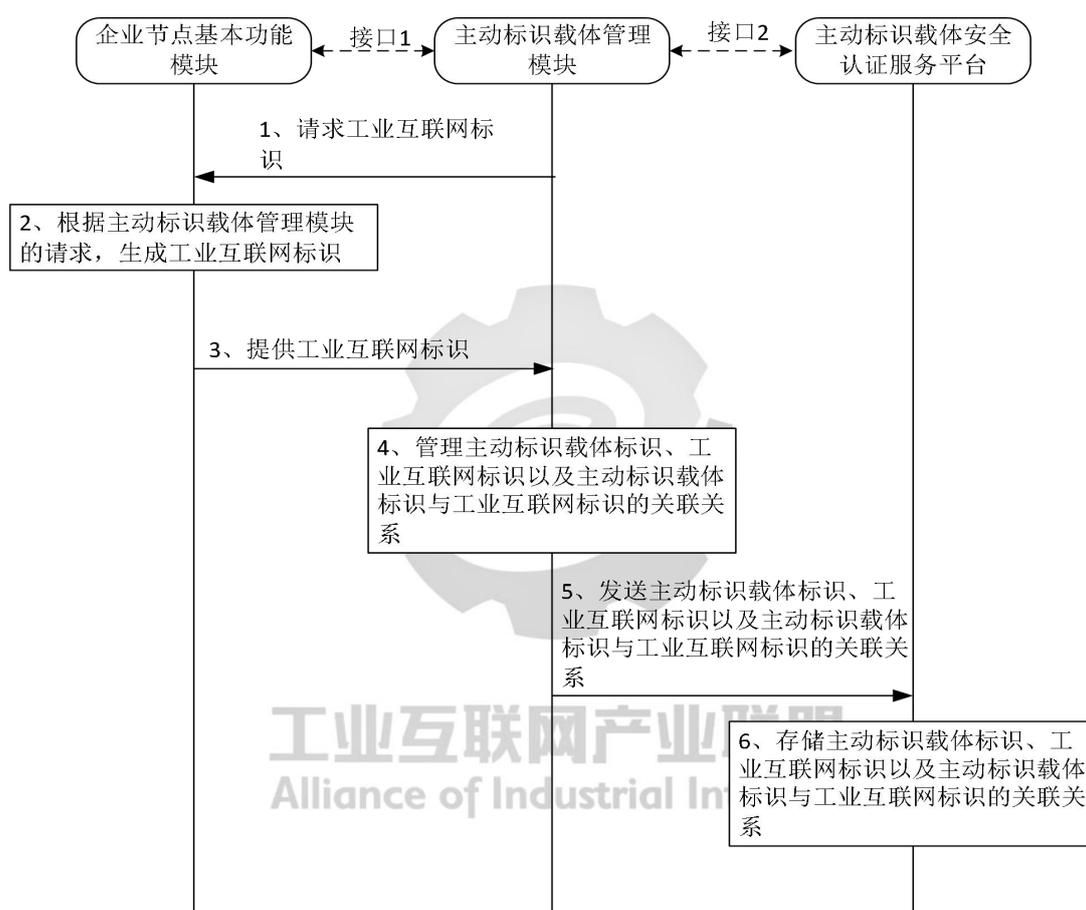


图3 主动标识载体安全认证服务平台获得工业互联网标识的流程示例

图3流程说明如下：

- (1) 主动标识载体管理模块向企业节点基本功能模块请求工业互联网标识；
- (2) 企业节点基本功能模块根据主动标识载体管理模块的请求生成工业互联网标识；
- (3) 企业节点基本功能模块向主动标识载体管理模块提供工业互联网标识；
- (4) 主动标识载体管理模块管理主动标识载体标识、工业互联网标识以及主动标识载体标识与工业互联网标识的关联关系；
- (5) 主动标识载体管理模块管理将主动标识载体标识、工业互联网标识、以及主动标识载体标识与工业互联网标识的关联关系发送给主动标识载体安全认证服务平台；
- (6) 主动标识载体安全认证服务平台存储主动标识载体标识、工业互联网标识以及主动标识载体标识与工业互联网标识的关联关系。

8.3.2 核心流程

主动标识载体管理模块通过主动标识载体安全认证服务平台向主动标识载体写入工业互联网标识的流程见图4。

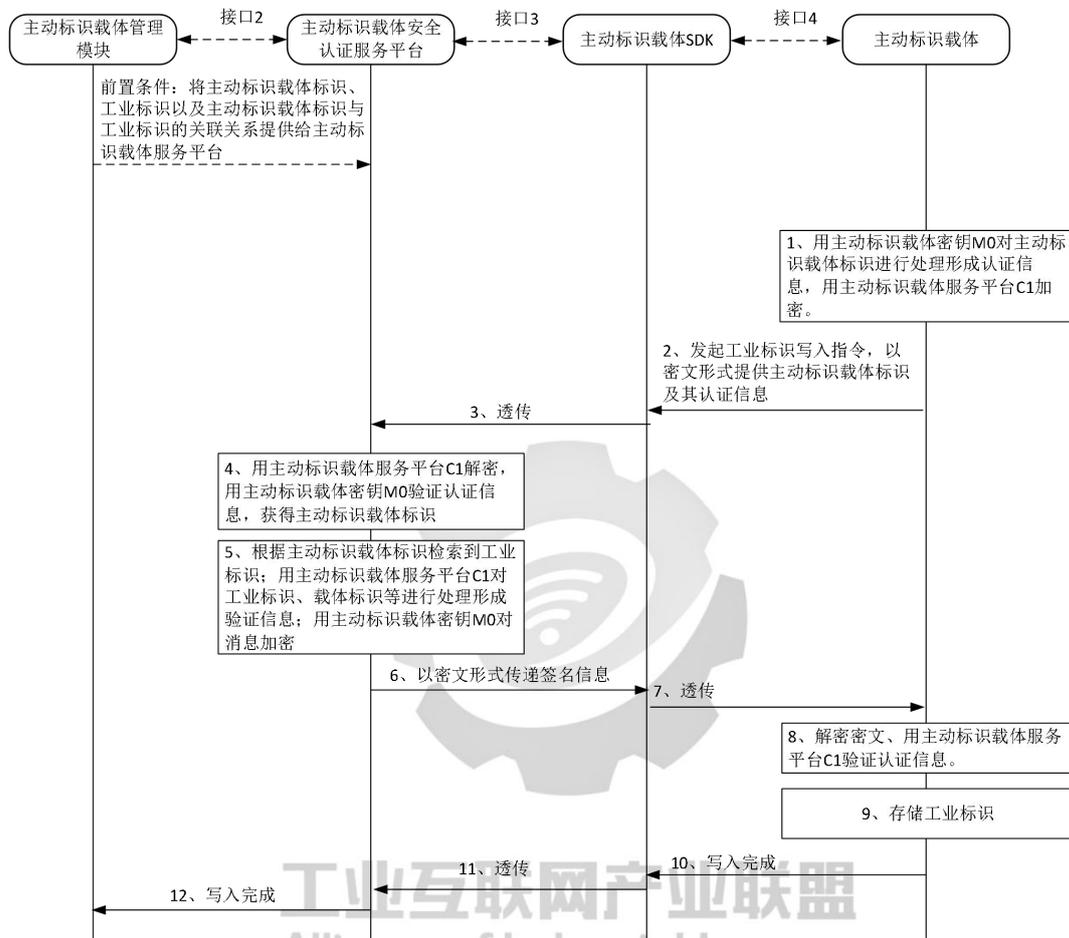


图4 主动标识载体管理模块通过主动标识载体安全认证服务平台向主动标识载体写入工业互联网标识的流程示例

图4流程说明如下：

(1) 主动标识载体宜用密钥M0对主动标识载体标识进行处理，形成认证信息，并宜用主动标识载体安全认证服务平台凭证C1对该认证信息加密；

(2) 主动标识载体应发起工业互联网标识写入主动标识载体的流程，并宜以密文形式将主动标识载体标识及其认证信息发给主动标识载体SDK；

(3) 主动标识载体SDK应将主动标识载体标识及其认证信息的密文发送给主动标识载体安全认证服务平台；

(4) 主动标识载体安全认证服务平台应用凭证C1解密密文，应用密钥M0验签认证信息，获得主动标识载体标识；

(5) 主动标识载体安全认证服务平台应依据主动标识载体标识以及主动标识载体与工业互联网标识之间的关联关系获得工业互联网标识；应用凭证C1对工业互联网标识、主动标识载体标识等信息进行处理形成认证信息；应用主动标识载体密钥M0对工业互联网标识、主动标识载体标识以及认证信息加密；

(6) 主动标识载体安全认证服务平台应以密文形式将工业互联网标识、主动标识载体标识以及认证信息发给主动标识载体SDK；

(7) 主动标识载体SDK应将工业互联网标识、主动标识载体标识以及认证信息的密文透传给主动标识载体；

(8) 主动标识载体应采用凭证C1的解密密文，并采用密钥M0验证认证信息；

(9) 验签通过后，主动标识载体应存储该工业互联网标识；

(10) 主动标识载体应用M0对写入操作结果信息进行处理形成认证信息、宜用凭证C1对写入操作结果信息以及认证信息加密后，将密文发送给主动标识载体SDK；

(11) 主动标识载体SDK应将步骤（10）生成的密文透传给主动标识载体安全认证服务平台；

(12) 主动标识载体安全认证服务平台用凭证C1解密，用M0验证认证信息，从而获得写入操作结果信息，再将写入操作结果信息发送给主动标识载体管理模块”。

8.4 主动标识载体管理模块通过主动标识载体安全认证服务平台从主动标识载体读取工业互联网标识

8.4.1 前置条件

本流程的前置流程见8.3。

8.4.2 核心流程

主动标识载体管理模块通过主动标识载体安全认证服务平台从主动标识载体读取工业互联网标识的流程见图5。

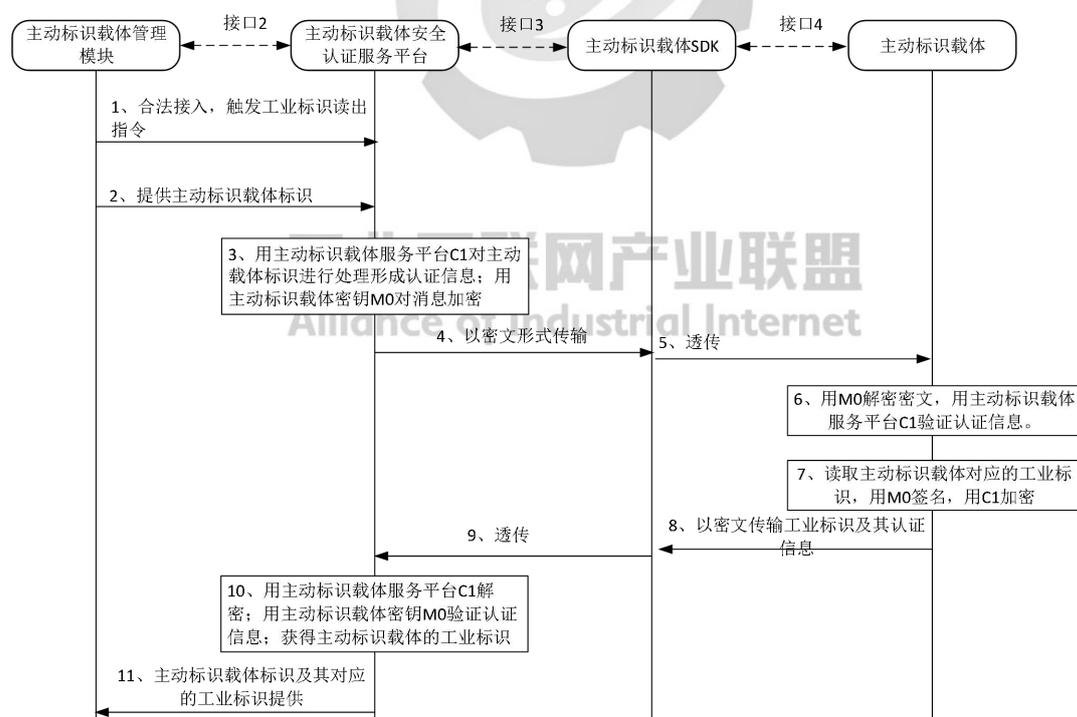


图5 主动标识载体管理模块通过主动标识载体安全认证服务平台从主动标识载体读取工业互联网标识的流程示例

图5流程说明如下：

(1) 主动标识载体管理模块向主动标识载体安全认证服务平台触发工业互联网标识读取流程；

(2) 主动标识载体管理模块将对应的主动标识载体标识、读取操作指令等发送给主动标识载体安全认证服务平台；

(3) 主动标识载体安全认证服务平台用凭证C1对主动标识载体标识、读取指令等进行处理，形成认证信息，用主动标识载体密钥M0对主动标识载体标识、读取指令及其认证信息加密，形成密文；

(4) 主动标识载体安全认证服务平台将密文发送给主动标识载体SDK；

(5) 主动标识载体SDK将密文透传给主动标识载体；

(6) 主动标识载体用M0解密密文，用主动标识载体安全认证服务平台凭证C1验证认证信息；

(7) 主动标识载体执行读取工业互联网标识操作，用主动标识载体密钥M0对工业互联网标识等信息进行处理，形成认证信息，用凭证C1对工业互联网标识及其认证信息等加密；

(8) 主动标识载体将工业互联网标识及其认证信息等以密文形式发给主动标识载体SDK；

(9) 主动标识载体SDK将密文透传给主动标识载体安全认证服务平台；

(10) 主动标识载体安全认证服务平台用凭证C1解密，用M0验证认证信息，从而获得主动标识载体的工业互联网标识；

(11) 主动标识载体安全认证服务平台将主动标识载体标识及其对应的工业互联网标识发送给主动标识载体管理模块。

8.5 主动标识载体管理模块通过主动标识载体安全认证服务平台删除主动标识载体中的工业互联网标识

8.5.1 前置条件

本流程的前置流程见8.3。

8.5.2 核心流程

主动标识载体管理模块通过主动标识载体安全认证服务平台删除主动标识载体中的工业互联网标识的流程见图6。

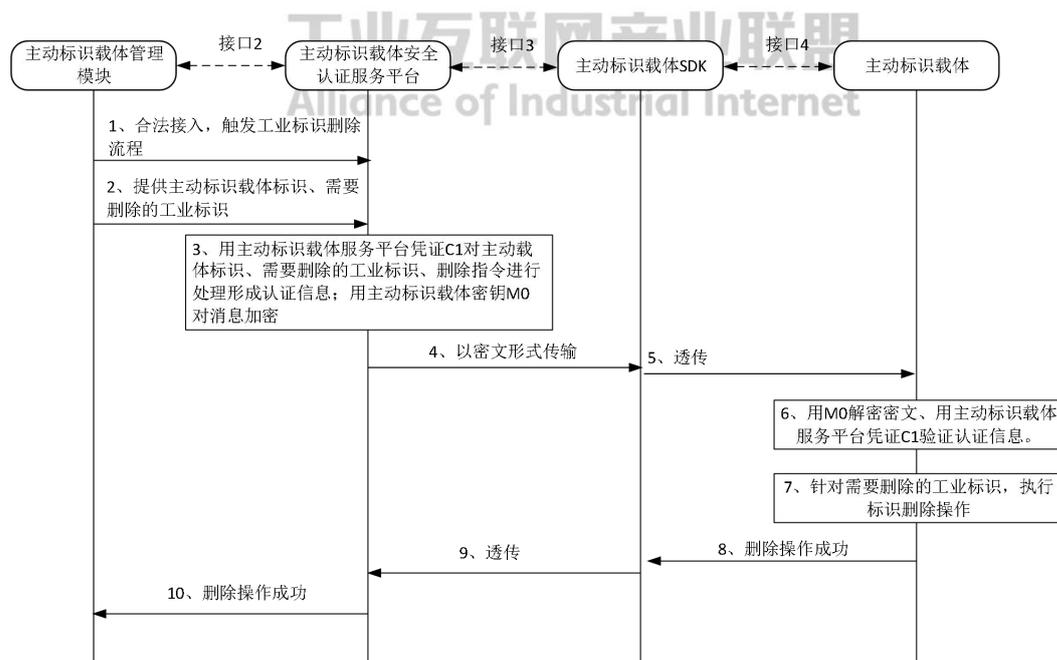


图6 主动标识载体管理模块通过主动标识载体安全认证服务平台删除主动标识载体中的工业互联网标识

识示例

图6流程说明如下：

- (1) 主动标识载体管理模块触发工业互联网标识删除流程；
- (2) 主动标识载体管理模块将待删除的工业互联网标识及其对应的主动标识载体标识、删除操作指令等发送给主动标识载体安全认证服务平台；
- (3) 主动标识载体安全认证服务平台用凭证C1对主动标识载体标识、待删除的工业互联网标识、删除指令等进行处理，形成认证信息；用M0对主动标识载体标识、待删除的工业互联网标识、删除指令及其认证信息加密，形成密文；
- (4) 主动标识载体安全认证服务平台将密文发送给主动标识载体SDK；
- (5) 主动标识载体SDK将密文透传给主动标识载体；
- (6) 主动标识载体用密钥M0解密密文，用凭证C1验证认证信息；
- (7) 主动标识载体根据删除指令删除待删除的工业互联网标识；
- (8) 主动标识载体用M0对删除操作结果信息进行处理形成认证信息、用凭证C1对删除操作结果信息以及认证信息加密后，将密文发送给主动标识载体SDK；
- (10) 主动标识载体SDK将步骤（8）生成的密文透传给主动标识载体安全认证服务平台；
- (11) 主动标识载体安全认证服务平台将删除操作成功的消息发送给主动标识载体管理模块。主动标识载体安全认证服务平台用凭证C1解密，用M0验证认证信息，从而获得删除操作结果信息，再将删除操作结果信息发送给主动标识载体管理模块”

8.6 主动标识载体管理模块通过主动标识载体安全认证服务平台修改主动标识载体中的工业互联网标识

8.6.1 前置条件

本流程的前置流程见8.3。

8.6.2 核心流程

主动标识载体管理模块通过主动标识载体安全认证服务平台修改主动标识载体中的工业互联网标识的核心流程参见8.3。

8.7 终端工业应用 APP 读取主动标识载体中的工业互联网标识

8.7.1 前置条件

本流程的前置流程见8.3。

8.7.2 核心流程

终端工业应用APP读取主动标识载体中工业互联网标识的流程见图7。

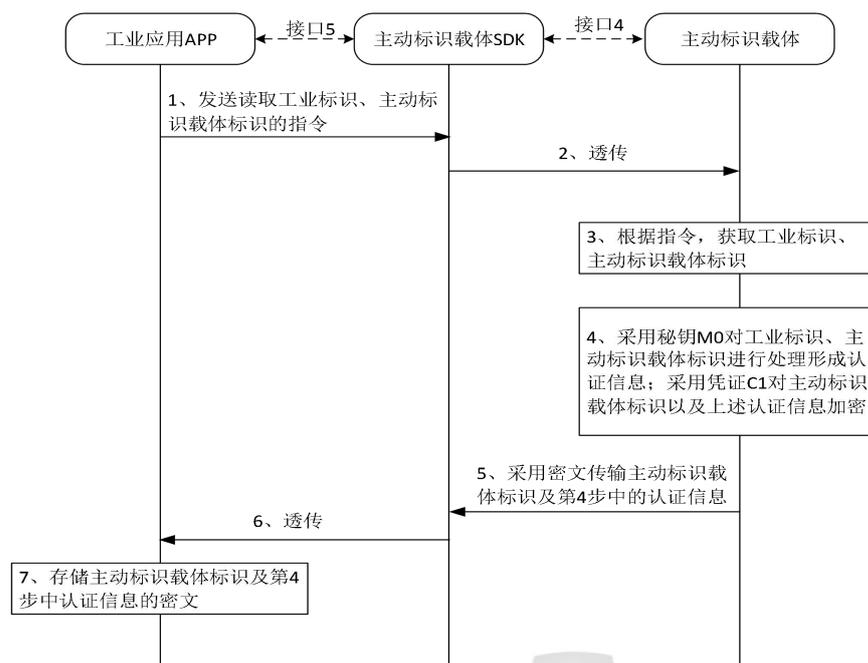


图7 工业应用 APP 读取主动标识载体中工业互联网标识的流程示例

图7流程说明如下：

- (1) 工业应用APP向主动标识载体SDK发送读取工业互联网标识、主动标识载体标识的指令；
- (2) 主动标识载体SDK将从流程（1）收到的指令透传给主动标识载体；
- (3) 主动标识载体根据读取工业互联网标识、主动标识载体标识的指令，获取工业互联网标识、主动标识载体标识；
- (4) 主动标识载体采用主动标识载体的密钥M0对工业互联网标识和主动标识载体标识进行处理，形成认证信息；可采用凭证C1的公钥对主动标识载体标识及上述认证信息加密，形成密文；
- (5) 主动标识载体将密文、工业互联网标识、主动标识载体标识等信息发给主动标识载体SDK；
- (6) 主动标识载体SDK将密文、工业互联网标识、主动标识载体标识等信息发送给工业应用APP；
- (7) 工业应用APP存储工业互联网标识、主动标识载体标识及（4）中认证信息的密文。

注1：终端工业应用APP读取通用集成电路卡中的工业互联网标识的具体流程和要求见《工业互联网标识解析 主动标识载体 通用集成电路卡技术要求》。

注2：终端工业应用APP读取安全芯片中的工业互联网标识的具体流程和要求见《工业互联网标识解析 主动标识载体 安全芯片技术要求》。

注3：终端工业应用APP读取通信模组中的工业互联网标识的具体流程和要求见《工业互联网标识解析 主动标识载体 通信模组技术要求》。

8.8 基于主动标识载体的主动数据上报

8.8.1 前置条件

本流程的前置流程见8.3和8.7。

8.8.2 核心基本流程

工业终端基于主动标识载体的主动数据上报流程见图8。

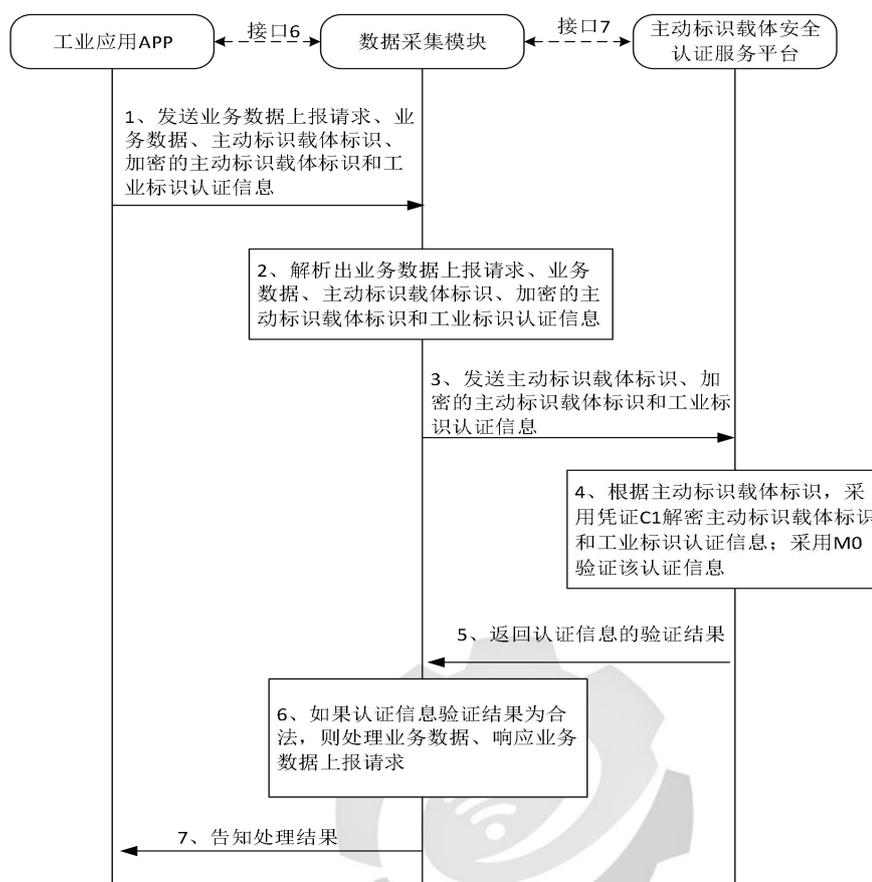


图8 基于主动标识载体的主动数据上报的流程示例

图8的流程说明如下：

- (1) 工业应用APP向数据采集模块发送业务数据上报请求，该请求应包括业务数据、主动标识载体标识、工业互联网标识、加密密文（包括主动标识载体标识、工业互联网标识和认证信息等）；
- (2) 数据采集模块解析出业务数据上报请求，该请求应包括业务数据、主动标识载体标识、工业互联网标识、加密密文（包括主动标识载体标识、工业互联网标识和认证信息等）；
- (3) 数据采集模块宜将主动标识载体标识、加密密文（包括主动标识载体标识、工业互联网标识和认证信息等）发送给主动标识载体安全认证服务平台；
- (4) 根据主动标识载体标识，主动标识载体安全认证服务平台采用凭证C1解密主动标识载体标识和工业互联网标识认证信息；并采用主动标识载体的密钥M0验证主动标识载体标识和工业互联网标识认证信息；
- (5) 主动标识载体安全认证服务平台将认证信息的验证结果返回数据采集模块；
- (6) 如果认证信息的验证结果为合法，数据采集模块处理工业应用APP发来的业务数据，并响应工业应用APP的业务数据上报请求；
- (7) 数据采集模块将处理结果反馈给工业应用APP。

附录 A

(资料性附录)

资料性附录

主动标识载体在电梯监控场景中的应用示例

1 业务描述

电梯与居民的生命财产息息相关。政府有关部门、维保单位、电梯厂家、业主单位等都需要对电梯的运行状态进行监控。

一般情况下，电梯监控所依赖的信息系统（以下简称“电梯监控系统”）主要涉及轿厢上部的电梯数据采集终端（以下简称“电梯终端”）、电梯数据采集平台以及该平台与政府监管、维保单位、电梯厂家、业主单位的对接。

2 应用开发方案

采用5G室分等方案覆盖轿厢电梯井，用以支持视频、语音、监控数据的无线传输。主动标识载体技术在电梯监控场景中的应用开发方案，见图A.1。

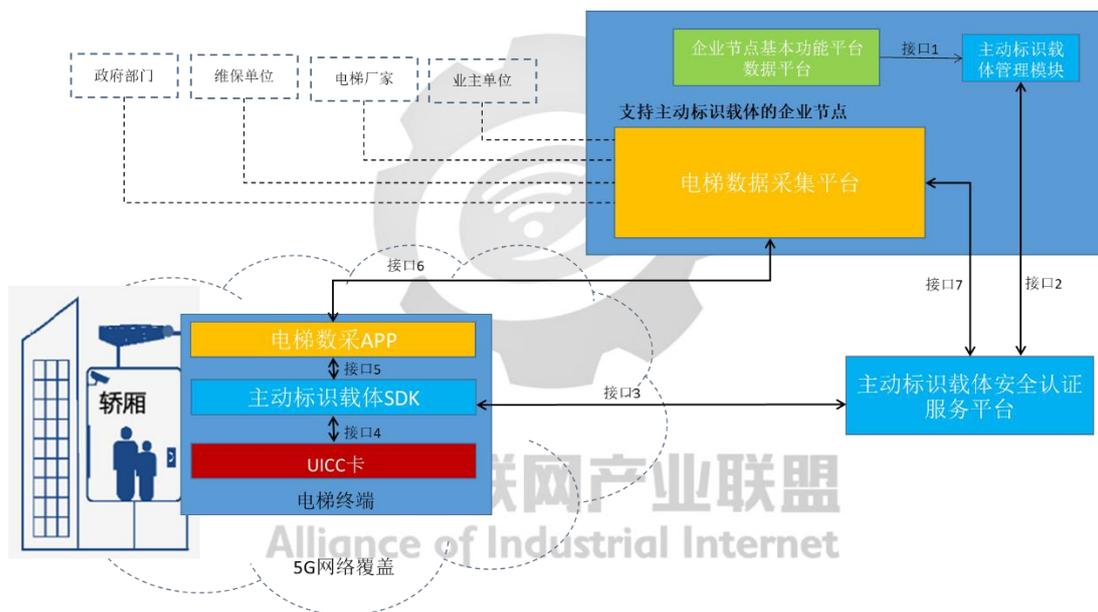


图 A.1 主动标识载体在电梯监控场景中的应用

(1) 电梯终端开发

- a. 5G模组提供商根据主动标识载体标准开发接口4和接口3的功能和协议，提供接口5。
- b. 电梯终端提供商将5G模组、主动标识载体UICC卡集成到5G电梯终端中。

(2) 电梯监控系统集成

电梯监控系统提供商集成5G电梯终端和电梯数据采集平台、开发5G终端侧的电梯数据APP。主要开发工作包括：

- a. 电梯数采APP：开发接口5和接口6对应的功能和协议；
- b. 电梯数据采集平台：开发接口7对应的功能和协议。

(3) 电梯监控系统运营准备

- a. 电梯监控系统运营方需向工业互联网标识解析二级节点申请支持主动标识载体的企业节点。

- b. 电梯监控系统运营方获得主动标识载体安全认证服务平台的服务：
 - i. 从主动标识载体安全认证服务平台获得主动标识载体管理模块；
 - ii. 获得激活接口1和接口2。
 - c. 电梯监控系统运营方从电梯监控系统提供商获得5G电梯终端以及电梯数据采集平台，并激活接口3、接口4、接口5、接口6和接口7。
-



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