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/021-2021

工业互联网标识解析 主动标识载体 安全认证技术要求

Industrial Internet identification resolution—Active identification carrier—technical requirements for security certification

工业互联网产业联盟

（2021 年 12 月 30 日发布）

目　　次

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标准。

标准牵头单位：中国信息通信研究院
标准起草单位和主要起草人：
——中国信息通信研究院：尹子航、刘澍、刘巍、谢滨、朱斯语、马宝罗、田娟、池程
——中国联合网络通信有限公司：贾雪琴
——联通华盛通信有限公司：孙阳阳
——中移物联网有限公司：柳耀勇、习熹
——紫光国芯微电子股份有限公司：霍航宇
——紫光展锐(上海)科技有限公司：张伟强
——中国电信集团有限公司：那中丽、刘伟、刘洁
——郑州信大捷安信息技术股份有限公司：刘献伦、刘为华
——华为技术有限公司：张婷、潘伟、郑秀丽、江伟玉
——四川天邑康和通信股份有限公司：宋晓杰

工业互联网标识解析 主动标识载体 安全认证技术要求

1 范围

本文件规定了主动标识载体接入工业互联网标识解析体系的安全认证技术要求以及对主动标识载体的管理要求，包括能力要求、业务流程、通信协议、接口指令等。

本文件适用于工业互联网标识解析体系中主动标识载体安全认证服务的设计、开发、建设和运营等，并指导主动标识载体接入工业互联网标识解析体系。

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 20518-2018 信息安全技术 公钥基础设施 数字证书格式规范

GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907-2016 信息安全技术 SM4 分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35276-2017 信息安全技术 SM2 密码算法使用规范

GB/T 38635（所有部分） 信息安全技术 SM9 标识密码算法

GM/Z 4001 密码术语

3 术语、定义和缩略语

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1 术语和定义

3.1.1

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。

3.1.2

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）。

3.1.3

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。

3.2 缩略语

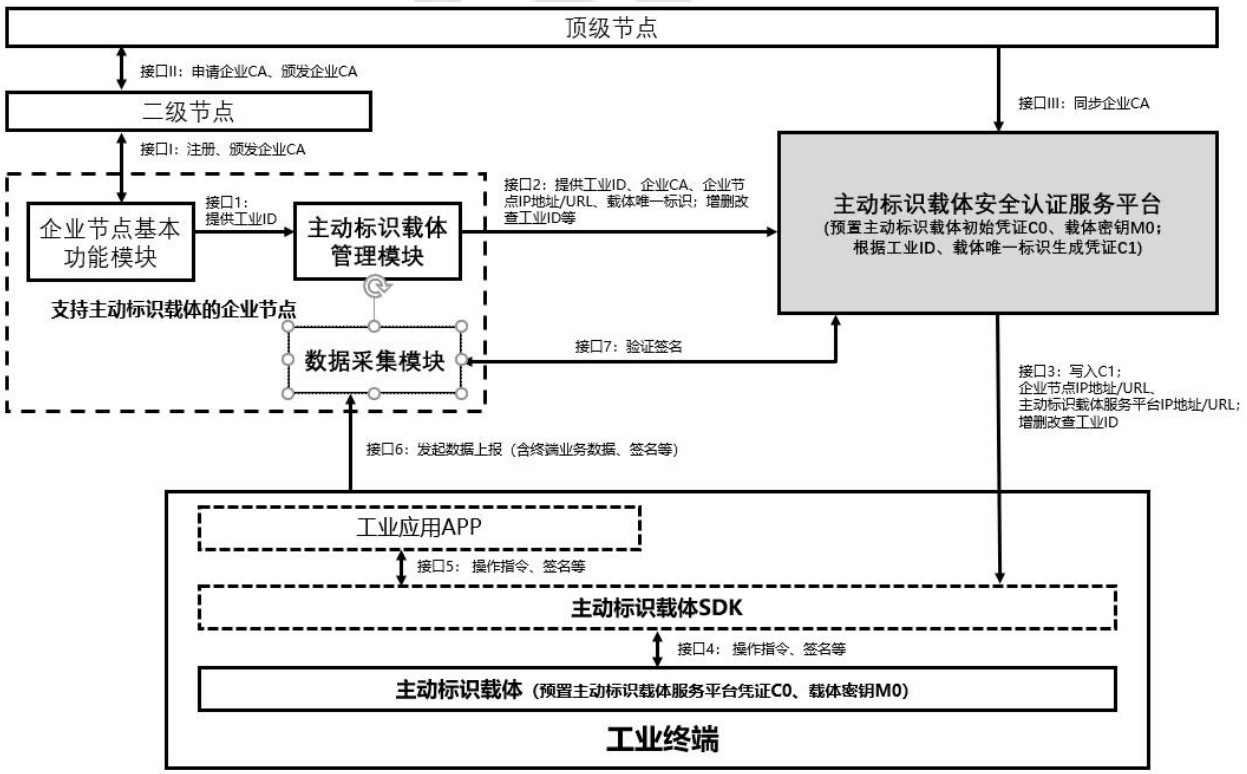
下列缩略语适用于本文件。

AES 高级加密标准（Advanced Encryption Standard）

CA	证书颁发机构（Certificate Authority）
CoAP	受限应用协议（the Constrained Application Protocol）
ECC	椭圆曲线加密算法（Elliptic curve cryptography）
HTTPS	安全套接字层超文本传输协议（Hyper Text Transfer Protocol over SecureSocket Layer）
MQTT	消息队列遥测传输协议（Message Queue Telemetry Transport）
RSA	由三个发明者姓氏首字母命名的公钥加密算法（Rivest-Shamir-Adleman）
SDK	软件开发工具包（Software Development Kit）
SHA	安全散列算法（Secure Hash Algorithm）
TDES	三重数据加密标准（Triple DES）

4 主动标识载体安全认证技术概述

主动标识载体总体技术架构参照《工业互联网标识解析 主动标识载体 总体技术框架》，总体技术架构见图1，包括主动标识载体、工业终端（含主动标识载体SDK）、主动标识载体管理模块、主动标识载体安全认证服务平台、数据采集模块、支持主动标识载体的企业节点、顶级节点、二级节点之间的数据交互及逻辑关系。



注：工业ID 是工业互联网标识的简称。

图1 主动标识载体总体技术架构以及安全认证服务的范围和接口

主动标识载体安全认证服务至少支持千万级并发接入，通过对具有主动标识载体的工业终端进行凭证管理、标识管理以及安全服务，提升工业基础设施的安全能力，保障标识数据和解析行为的安全。主动标识载体安全认证服务模块负责对接工业互联网顶级节点、企业节点的主动标识载体管理模块、数据采集模块及工业终端中的主动标识载体SDK。

（1）与顶级节点信息对接，负责接收顶级节点同步的企业信息及CA证书；

（2）与企业节点的主动标识载体管理模块对接，负责接收模块请求，对主动标识载体中的工业互联网标识进行增、删、改、查等操作、对企业工业终端的主动标识载体进行标识管理、凭证管理、以及为企业提供安全服务；

（3）与数据采集模块交互，负责接收主动标识载体的身份验证申请，并反馈验证结果；

（4）与工业终端中的主动标识载体SDK对接，将工业互联网标识、主动标识载体标识、企业节点CA、企业节点IP地址或者URL等信息写入到主动标识载体中。

5 主动标识载体安全认证技术能力要求

主动标识载体安全认证技术能力要求主要包括基本能力、安全能力、通信能力，具体见图2。

图2 主动标识载体安全认证技术能力要求

主动标识载体安全认证技术能力要求具体包括：

（1）基本能力应包括但不限于：主动标识载体标识与工业互联网标识关联关系管理、企业CA证书管理、主动标识载体凭证管理、设备管理、密钥管理、指令管理、算法管理等；

（2）安全能力应包括但不限于： RSA、AES、SHA256、TDES、ECC、SM2、SM3、SM4、SM9等；

（3）通信能力应支持 MQTT、COAP 和 HTTPS等通信方式两种以上；

6 主动标识载体安全认证技术业务流程

6.1 同步企业 CA 证书

顶级节点向主动标识载体安全认证服务平台同步企业CA证书流程见图3，具体如下:

（1）支持主动标识载体的企业节点向二级节点注册并申请企业CA证书；

（2）二级节点向顶级节点申请颁发企业CA证书；

（3）顶级节点将企业CA证书返回给二级节点，同步企业CA证书给主动标识载体安全认证服务平台；

（4）二级节点将企业CA证书返回给支持主动标识载体的企业节点；

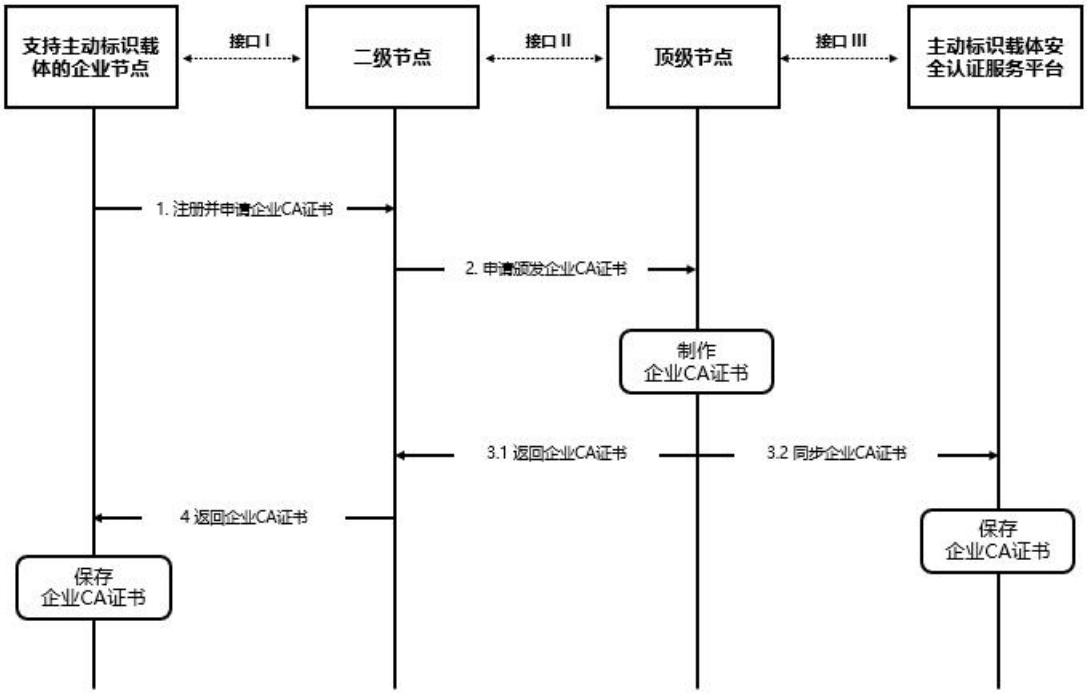


图3 顶级节点同步企业CA证书给主动标识载体安全认证服务平台

6.2 主动标识载体注册流程

主动标识载体首次上电向主动标识载体安全认证服务平台发起注册的流程见图4，具体如下：

前置条件：主动标识载体管理模块将工业互联网标识提供给主动标识载体安全认证服务平台。

（1）主动标识载体首次上电激活，采用主动标识载体密钥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主动标识载体密钥M0解密密文，获得凭证C1生成指令、主动标识载体等信息，完成主动标识载体标识与工业互联网标识的绑定，并存储在主动标识载体安全认证服务平台；

（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C或者密码散列算法生成的身份指纹；

（6）主动标识载体安全认证服务平台采用主动标识载体初始凭证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，同时返回工业互联网标识与主动标识载体标识的关联关系信息给主动标识载体管理模块；

（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；采用主动标识载体初始凭证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。

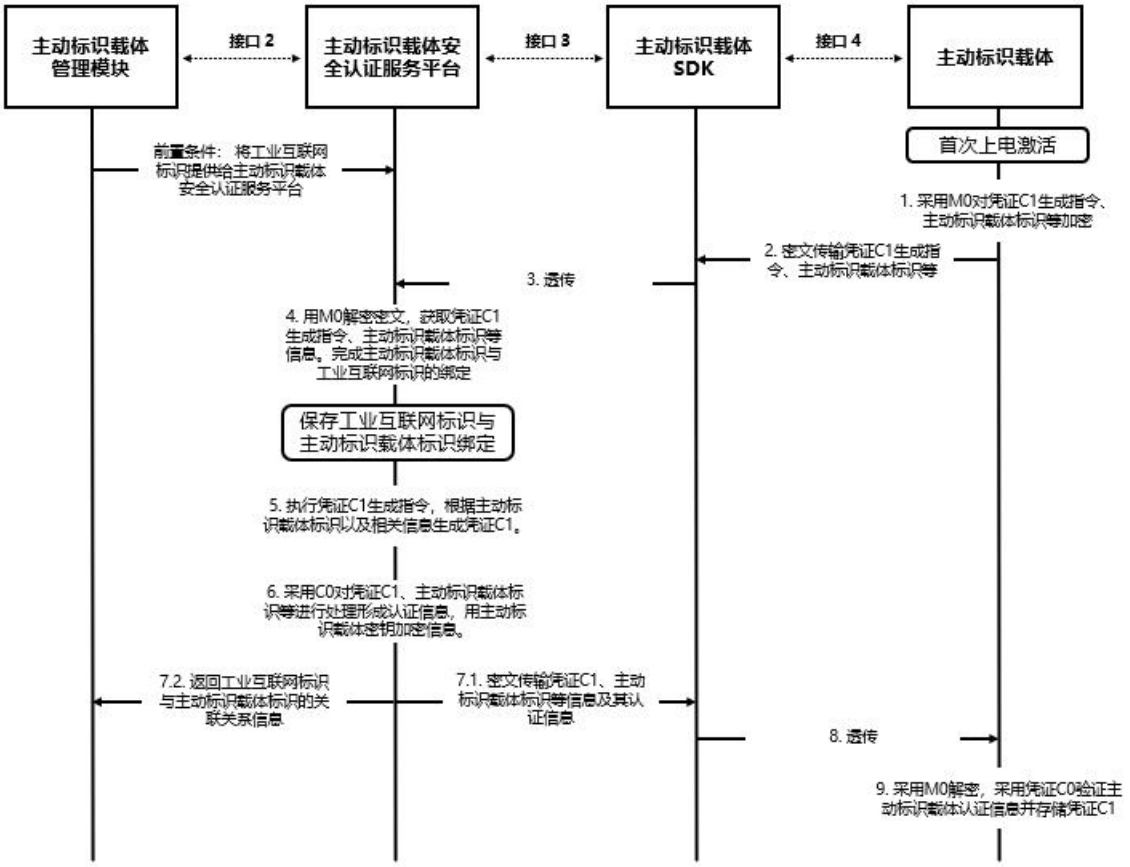


图4 主动标识载体注册流程

6.3 主动标识载体身份认证

本流程前置流程参见6.2。

工业终端基于主动标识载体的数据上报中主动标识载体身份认证流程见图5，具体如下：

（1）主动标识载体上报数据信息，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；并采用凭证C1对主动标识载体标识及上述认证信息加密，形成密文；

（2）主动标识载体将密文发给主动标识载体SDK；

（3）主动标识载体SDK将密文透传给工业应用APP，工业应用APP存储主动标识载体及（1）中认证信息的密文；

（4）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、加密的主动标识载体标识和工业互联网标识认证信息。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、加密的主动标识载体标识和工业互联网标识认证信息；

（5）数据采集模块将主动标识载体标识、加密的主动标识载体标识和工业互联网标识认证信息发送给主动标识载体安全认证服务平台。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；

（6）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，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APA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。

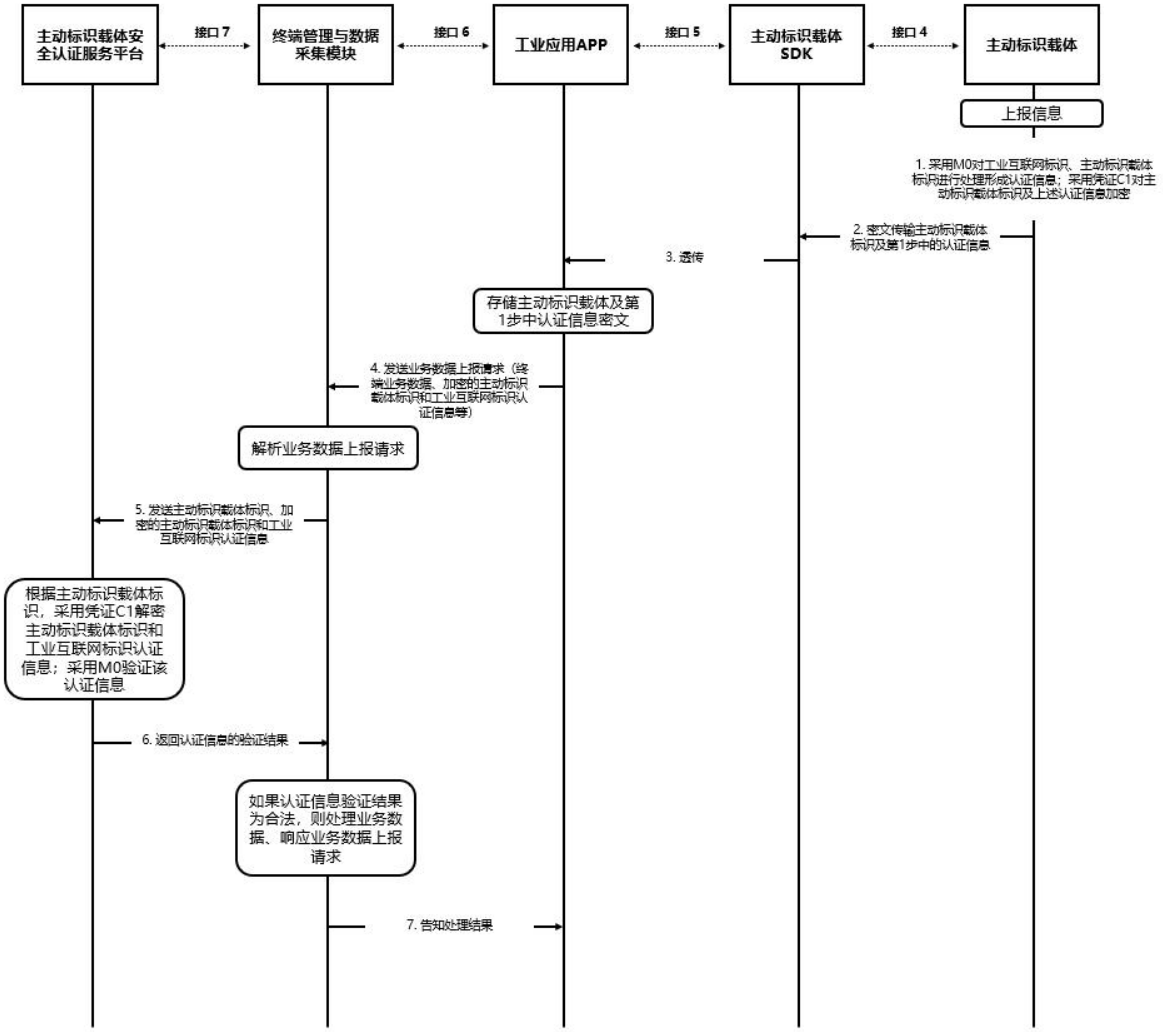


图5 主动标识载体身份认证

6.4 主动标识载体管理业务

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发起工业互联网标识管理业务，主动标识载体安全认证服务平台通过主动标识载体SDK完成实现对主动标识载体的工业互联网标识的增、删、改、查等操作。

附　录 A

（规范性）

主动标识载体安全认证技术通信协议

A.1 与主动标识载体管理模块及数据采集模块通信

A.1.1 上电激活

请求路径：/api/loongxy-security/securityV2/active
请求方式：post

请求参数见表A.1，响应参数见A.2。

表A.1 请求参数表

字段	名称	类型	必填
appId	应用ID（平台分配）	String	Y
callback	回调地址	String	Y
identity	工业互联网标识	String	Y
noncr	随机数	String	Y
pubkey	终端公钥	String	Y
terminalNo	终端唯一编码	String	Y
timestamp	时间戳	String	Y
sign	签名	String	Y

图A.2 响应参数表

字段	名称	类型	必填
code	状态码（200:成功）	String	Y
success	是否成功	Boolean	Y
data	返回数据	String	N

msg	返回消息	String	Y

A.1.2 数据验签

请求路径：/api/loongxy-security/securityV2/verify
请求方式：post
请求参数见 A.3，响应参数见 A.4。

表 A.3 请求参数表

字段	名称	类型	必填
appId	应用ID（平台分配）	String	Y
encryptMsg	签名密文	String	Y
noncr	随机数	String	Y
plainTxt	签名明文	String	Y
terminalNo	终端唯一编码	String	Y
timestamp	时间戳	String	Y
sign	签名	String	Y

表 A.4 请求参数响应参数表

字段	名称	类型	必填
code	状态码（200:成功）	String	Y
success	是否成功	Boolean	Y
data	返回数据	String	N
msg	返回消息	String	Y

A.1.3 指令下发

请求路径：/api/loongxy-security/securityV2/command
请求方式：post
请求参数见表 A.5,请求参数响应参数见表 A.6。

A.5 请求参数表

字段	名称	类型	必填
appId	应用ID（平台分配）	String	Y
callback	回调地址	String	Y
data	请求数据	String	N
noncr	随机数	String	Y
reqType	请求类型 0101：烧录CA 0102：删除CA 0201：数据签名 0202：数据验签 0203：数据加密 0204：数据解密 0301：标识写入 0302：标识读取 0303：标识修改 0304：标识删除	String	Y
terminalNo	终端唯一编码	String	Y
timestamp	时间戳	String	Y
sign	签名	String	Y

A.6 响应参数表

字段	名称	类型	必填
code	状态码（200:成功）	String	Y
success	是否成功	Boolean	Y
data	返回数据	String	N
msg	返回消息	String	Y

A.2 与主动标识载体通信

A.2.1 调用主动标识载体接口

请求数据格式见图 A.1，响应数据格式见图 A.2.

请求参数见表 A.6,相应参数见表 A.7。

图 A.1 数据格式

A.6 请求参数表

字段	占用字节数	备注
请求头	1字节	请求头固定0x80
指令类别	1字节	指令代表操作的对象
指令操作	1字节	指令对象的具体操作
身份标识	8字节	安全管理平台唯一识别号加密后的结果
数据长度	2字节	代表报文最后对数据加密后的长度
数据	N字节	需要发送的数据

图 A.2 响应数据格式

A.7 响应参数表

字段	占用字节数	备注
响应头	1字节	响应头固定0x90
指令类别	1字节	指令代表操作的对象
指令操作	1字节	指令对象的具体操作
身份标识	8字节	安全管理平台唯一识别号加密后的结果
处理结果	1字节	成功00，失败01
数据长度	2字节	代表报文最后对数据加密后的长度
数据	N字节	需要发送的数据

A.2.2 载体凭证烧录

功能描述，将CA烧录进标识载体终端。

请求参数见表A.8,响应参数见A.9，命令格式见表A.10。

A.8 响应参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x01	0x01	平台唯一识别号	Len(数据)	证书公钥

A.9 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x01	0x01	平台唯一识别号	0x00	0	
0x90	0x01	0x01	平台唯一识别号	0x01	Len(数据)	失败原因

A.10 命令格式

协议	命令	备注

MQTT	AT	
COAP	coap://ip:port/writeca	Method: POST
HTTPS	https://ip:port/writeca	Method: POST

A.2.3 载体凭证删除

功能描述：执行载体凭证删除。

请求参数见表A.11,响应参数见A.12，命令格式见表A.13。

表A.11 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x01	0x02	E(平台唯一识别号)	0	

表A.12 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x01	0x02	E(平台唯一识别号)	0x00	0	
0x90	0x01	0x02	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.13 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/delca	Method: DELETE
HTTPS	https://ip:port/delca	Method: DELETE

A.2.4 数字签名

功能描述：执行标识数据签名。

请求参数见表A.14，响应参数见A.15，命令格式见表A.16。

A.14 命令格式

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x02	0x01	E(平台唯一识别号)	Len（数据）	E(需签名的数据)

A.15 命令格式

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x02	0x01	E(平台唯一识别号)	0x00	Len(数据)	签名后的结果

A.15 （续）

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x02	0x01	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.16 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/signature	Method: POST
HTTPS	https://ip:port/signature	Method: POST

A.2.5 数字验签

功能描述：执行标识数据验签。

请求参数见表A.17，响应参数见A.18，命令格式见表A.19。

A.17 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x02	0x02	E(平台唯一识别号)	Len（数据）	E(签名)

A.18 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x02	0x02	E(平台唯一识别号)	0x00	0	
0x90	0x02	0x02	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.19 命令格式

协议	命令	备注

MQTT	AT	
COAP	coap://ip:port/verifysign	Method: POST

A.19 （续）

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/verifysign	Method: POST
HTTPS	https://ip:port/verifysign	Method: POST

A.2.6 数据加密

功能描述：执行标识数据加密。

请求参数见表A.20，响应参数见A.21，命令格式见表A.22。

A.20 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x02	0x03	E(平台唯一识别号)	Len（数据）	E(需加密的数据)

A.21 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x02	0x03	E(平台唯一识别号)	0x00	Len(数据)	加密后的结果
0x90	0x02	0x03	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.22 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/encrypt	Method: POST
MQTT	AT	
COAP	coap://ip:port/encrypt	Method: POST

HTTPS	https://ip:port/encrypt	Method: POST

A.2.7 数据解密

功能描述：执行标识数据解密。

请求参数见表A.23，响应参数见A.24，命令格式见表A.25。

A.24 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x02	0x04	E(平台唯一识别号)	Len（数据）	E(需解密的数据)

A.25 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x02	0x04	E(平台唯一识别号)	0x00	Len(数据)	解密后的结果
0x90	0x02	0x04	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.26 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/decrypt	Method: POST
HTTPS	https://ip:port/decrypt	Method: POST

A.2.8 标识写入

功能描述：执行标识写入，将工业标识写入通信模组的安全存储区。

请求参数见表A.27，响应参数见A.28，命令格式见表A.29。

A.27 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x03	0x01	E(平台唯一识别号)	Len（数据）	E(工业互联网标识)

A.28 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x03	0x01	E(平台唯一识别号)	0x00	0	
0x90	0x03	0x01	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.29 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/writeidentifier	Method: POST
HTTPS	https://ip:port/writeidentifier	Method: POST

A.2.9 标识读取

功能描述：执行标识读取。

请求参数见表A.30，响应参数见A.31，命令格式见表A.32。

A.30 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x03	0x02	E(平台唯一识别号)	0	

A.31响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x03	0x02	E(平台唯一识别号)	0x00	Len(数据)	E(读取的标识)
0x90	0x03	0x02	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.32 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/readidentifier	Method: POST

HTTPS	https://ip:port/readidentifier	Method: POST

A.2.10 标识修改

功能描述：执行标识修改。

请求参数见表A.33，响应参数见A.34，命令格式见表A.35。

A.33 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据
0x80	0x03	0x03	E(平台唯一识别号)	Len（数据）	E(工业互联网标识)

A.34 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x03	0x03	E(平台唯一识别号)	0x00	0	
0x90	0x03	0x03	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.35 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/modifyidentifier	Method: PUT
HTTPS	https://ip:port/modifyidentifier	Method: PUT

A.2.11 标识删除

功能描述：执行标识删除。

请求参数见表A.36，响应参数见A.37，命令格式见表A.38。

A.36 请求参数表

请求头	指令类别	指令操作	身份标识	数据长度	数据

0x80	0x03	0x04	E(平台唯一识别号)	0	

A.37 响应参数表

响应头	指令类别	指令操作	身份标识	处理结果	数据长度	数据
0x90	0x03	0x04	E(平台唯一识别号)	0x00	0	
0x90	0x03	0x04	E(平台唯一识别号)	0x01	Len(数据)	E(失败原因)

A.38 命令格式

协议	命令	备注
MQTT	AT	
COAP	coap://ip:port/delidentifier	Method: DELETE Payload: {at: AT}
HTTPS	https://ip:port/delidentifier	Method: DELETE Payload: {at: AT}