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/020-2021

工业互联网标识解析 主动标识载体通信模组技术要求

Industrial Internet identification resolution— Active identification carrier— Communication Module Technical Requirements

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。

本标准牵头单位：紫光国芯微电子股份有限公司

标准起草单位和主要起草人：

——紫光国芯微电子股份有限公司：霍航宇

——中国信息通信研究院：刘阳、刘澍、刘巍、田娟、谢滨、尹子航

——中国联合网络通信集团有限公司：贾雪琴，林晨，韩政鑫

——联通华盛通信有限公司：孙阳阳，韩梦梦

——联通智慧安全科技有限公司：姚韬、蒋小燕

——联通（黑龙江）产业互联网有限公司：吕威、李博鑫、张笑泳

——联通物联网有限责任公司：曹侃、张律、谢仁芳

——中移物联网有限公司：柳耀勇，肖青

——紫光同芯微电子有限公司：盛敬刚

——紫光展锐（上海）科技有限公司：张伟强

——郑州信大捷安信息技术股份有限公司：刘献伦

——广东省智能家电研究院：洪德欣

——苏州协同创新智能制造装备有限公司：袁雪腾

——佛山市联科发科技信息有限公司：许炜

——北京亚华物联科技发展有限公司：许长亮

——深圳市有方科技股份有限公司：方荣

工业互联网标识解析 主动标识载体 通信模组技术要求

1 范围

本文件规定了工业互联网标识解析主动标识载体的功能架构、能力要求、接口指令以及基本流程。

本文件适用于工业互联网中作为主动标识载体的通信模组。

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。

GM/T 0009-2012 SM2密码算法使用规范

GM/T 0015-2012 基于SM2密码算法的数字证书格式规范

GM/T 0003.1-2012 SM2椭圆曲线公钥密码算法 第1部分：总则

GM/T 0003.2-2012 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GM/T 0003.3-2012 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

GM/T 0003.4-2012 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

GM/T 0003.5-2012 SM2椭圆曲线公钥密码算法推荐曲线参数

GM/T 0004-2012 SM3密码杂凑算法

GM/T 0002-2012 SM4分组密码算法

GB4943.1-2011《信息技术设备安全第1部分：通用要求》

YD/T 2436.2-2018 多模移动终端电磁干扰技术要求和测试方法 第2部分：蜂窝无线模组与无线局域网间电磁干扰

2018-0177T-YD 面向蜂窝物联网的通用模组技术要求

2020-0008T-YD 5G通用模组技术要求（第一阶段）

2021-0598T-YD 5G通用模组技术要求（第二阶段）(征求意见稿)

3GPP TS27.007 AT command set for User Equipment (UE)

《工业互联网标识解析 主动标识载体 总体技术框架》

3 术语和定义

3.1 标识编码

标识编码 identifier 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

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

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。

4 缩略语

下列缩略语适用于本文件。

3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
AES	Advanced Encryption Standard	高级加密标准
AT	Attention	应用于设备与应用之间的连接与通信的指令
BSP	board support package	板级支持包
CoAP	the Constrained Application Protocol	受限应用协议
DES	Data Encryption Standard	数据加密标准
HAL	Hardware Abstract Layer	硬件抽象层
HSM	Hardware Security Module	硬件安全模块
IoT	Internet of Things	物联网
MQTT	Message Queue Telemetry Transport	消息队列遥测传输协议
OS	Operating System	操作系统
OTA	Over the AirTechnology	空中下载技术
RSA	Rivest-Shamir-Adleman	一种加密认证体系，由三个发明者姓氏首字母命名
SHA	Secure Hash Algorithm	安全散列算法
UTRA	Universal Terrestrial Radio Access	通用地面无线接入

5 主动标识载体 通信模组功能架构

本标准针对主动标识载体为通信模组时的模组基本能力要求、应用要求进行规定。

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安全认证服务平台、支持主动标识载体安全认证服务平台的标识管理、支持主动标识载体安全认证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。

基于通信模组的工业互联网主动标识载体的功能架构如图见表。

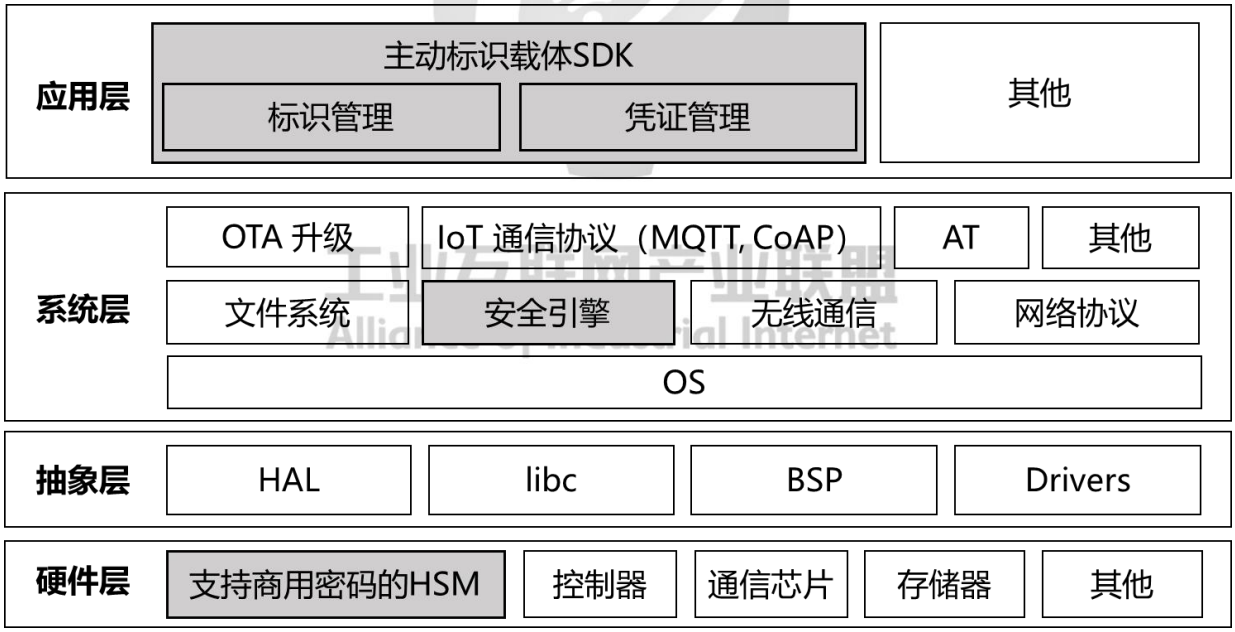

图1 用于主动标识载体的通信模组的功能架构图

如图1所示，主动标识载体通信模组主要包括：

硬件层，为安全承载工业互联网标识及其相应凭证，相对于常规通信模组，增加支持商用密码算法的HSM；

抽象层，与常规通信模组类似，由HAL、libc、BSP、Drivers等构成。

系统层，相对于常规通信模组，除了操作系统、文件系统、无线通信、网络协议、OTA升级、IoT通信协议（MQTT，CoAP）、AT等模块，增加SE安全引擎。

应用层，相对于常规通信模组，增加主动标识载体SDK，支持安全认证服务平台的标识管理与凭证管理，管理功能的具体指令详细描述请参见本规范第8章。

6 主动标识载体通信模组基本能力要求

6.1 支持通信网络连接

主动标识载体通信模组，应具备建立网络连接的能力，符合通用模组技术要求。

6.2 支持标识管理

应支持主动标识载体安全认证服务平台的身份凭证预置与OTA升级；

应支持与主动标识载体安全认证服务平台的信息交互；

应支持主动标识载体安全认证服务平台的标识写入、读取、修改与删除。

6.3 支持安全服务

1. 安全服务类别

应支持标识及其相应凭证的安全存储；

应支持与主动标识载体安全认证服务平台的身份认证；

应支持与主动标识载体安全认证服务平台的安全通信。

2. 安全能力要求

应支持多种加密算法模块，支持对称、非对称、摘要等算法，支持商用密码算法、国际算法，推荐商用密码算法。

对称算法：应支持AES，SM4等算法中的一种及以上；

非对称算法：应支持RSA、SM2等算法的一种及以上；

摘要算法：应支持SHA-256、SM3等算法中的一种及以上。

3. 安全认证要求

通信模组中的安全芯片应支持商用密码二级；

通信模组中的安全芯片应支持EAL4+及以上。

7 主动标识载体通信模组基本业务流程

7.1 信息交互框架

通信模组作为主动标识载体时，遵循《工业互联网标识解析主动标识载体总体技术框架》中的主动标识载体总体技术架构和接口，信息交互框架符合6.1中图1。

通信模组作为主动标识载体时，模块间的信息交互框架与《工业互联网标识解析主动标识载体总体技术框架》基本一致，支持主动标识载体的企业节点、主动标识载体安全认证服务平台、工业终端之间的框架简图如图见表。

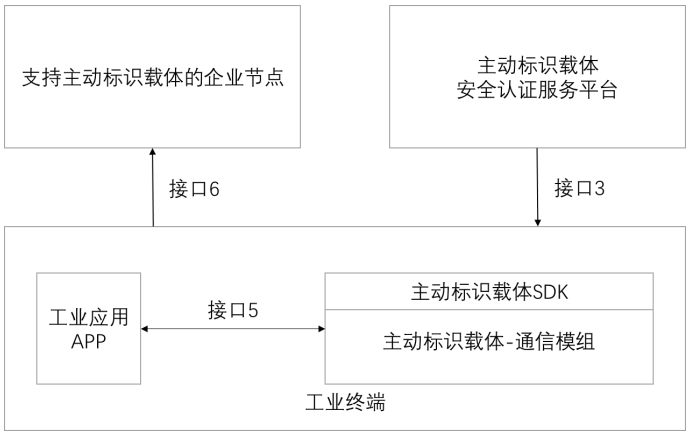

图 2 通信模组作为主动标识载体的信息交互框架

7.2 业务角色描述

支持主动标识载体的企业节点，角色定义及描述遵循《工业互联网标识解析 主动标识载体 总体技术框架》。

主动标识载体安全认证服务服务平台，角色定义及描述遵循《工业互联网标识解析 主动标识载体总体技术框架》和《工业互联网标识解析 主动标识载体 安全认证与管理技术要求》。

工业终端中的主动标识载体通信模组，应满足本标准要求的功能、性能要求，支持主动标识载体安全认证服务平台的标识管理和凭证管理，支持安全接入主动标识载体安全认证服务平台，支持工业互联网标识及其凭证的安全存储。

7.3 基本业务流程

相比于其他主动标识载体，通信模组作为主动标识载体时，主动标识载体SDK封装在通信模组内部，如图2所示，除此之外，基本业务流程遵循《工业互联网标识解析 主动标识载体 总体技术框架》。

8 主动标识载体通信模组接口命令

通信传输的AT命令，遵循3GPP TS27.007 AT command set for User Equipment (UE)。

图2中，接口5的AT命令，需具备如下功能。

8.1 凭证烧录

功能描述：将凭证烧录入主动标识载体。

8.2 凭证删除

功能描述：执行主动标识载体凭证删除。

8.3 标识写入

功能描述：将标识写入主动标识载体安全存储区。

8.4 标识读取

功能描述：从主动标识载体安全存储区读取工业标识。

8.5 标识删除

功能描述：将主动标识载体安全存储区的工业标识删除。

8.6 标识修改

功能描述：将主动标识载体安全存储区的工业标识ID修改。

8.7 身份签名

功能描述：读取主动标识载体的身份签名信息。

8.8 身份验签

功能描述：对平台/其他终端的身份合法性进行确认。

附 录A

（资料性附录）

通信模组遵循3GPP标准

NB及4G通信制式，应遵循如下3GPP标准。

TS36.101 (E-UTRA); User Equipment (UE) radio transmission and reception

TS36.133 (E-UTRA); Requirements for support of radio resource management

TS36.211 (E-UTRA) Physical Channels and Modulation

TS36.212 (E-UTRA) Multiplexing and Channel Coding

TS36.213 (E-UTRA) Physical layer procedures

TS36.214 (E-UTRA) Physical layer measurements

TS36.304 (E-UTRA); User Equipment (UE) procedures in idle mode

TS36.306 (E-UTRA); User Equipment (UE) radio access capabilities

TS36.321 (E-UTRA); Medium Access Control (MAC) protocol specification

TS36.322 (E-UTRA); Radio Link Control (RLC) protocol specification

TS36.323 (E-UTRA); Packet Data Convergence Protocol (PDCP) specification

TS36.331 (E-UTRA); Radio Resource Control (RRC); Protocol specification

TS36.509 E-UTRA) and (EPC); Special conformance testing functions for User Equipment (UE)

TS24.301 (NAS) protocol for Evolved Packet System (EPS); Stage 3

5G通信制式，应遵循如下3GPP标准。

TS38.101-1 NR; User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone

TS38.101-2 NR; User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone

TS38.101-3 NR; User Equipment (UE) radio transmission and reception; Part 3: Range 1 and Range 2 Interworking operation with other radios

TS38.101-4 NR; User Equipment (UE) radio transmission and reception; Part 4: Performance requirements

TS38.133 NR; Requirements for support of radio resource management

TS38.201 NR; Physical layer; General description

TS38.202 NR; Services provided by the physical layer

TS38.211 NR; Physical channels and modulation

TS38.212 NR; Multiplexing and channel coding

TS38.213 NR; Physical layer procedures for control

TS38.214 NR; Physical layer procedures for data

TS38.215 NR; Physical layer measurements

TS38.304 NR; User Equipment (UE) procedures in idle mode and in RRC Inactive state

TS38.305 NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN

TS38.306 NR; User Equipment (UE) radio access capabilities

TS38.307 NR; Requirements on User Equipment's (UEs) supporting a release-independent frequency band

TS38.321 NR; Medium Access Control (MAC) protocol specification
TS38.322 NR; Radio Link Control (RLC) protocol specification
TS38.323 NR; Packet Data Convergence Protocol (PDCP) specification
TS38.324 NR; Service Data Protocol (SDAP) specification
TS38.331 NR; Radio Resource Control (RRC); Protocol specification
TS38.509 5GS; Special conformance testing functions for User Equipment (UE)

附 录 B

（资料性附录）

主动标识载体通信模组 AT 命令

通信传输的AT命令，遵循3GPP TS27.007 AT command set for User Equipment (UE)。
作为工业互联网主动标识载体的通信模组，与工业互联网标识解析相关的AI命令，定义表见表B.1。

表 B.1 主动标识载体通信模组 AT 命令说明

序号	命令名称	命令类型	描述
1	AT+IIIDADDCERT	执行命令	凭证烧录
2	AT+IIIDDELCCERT	执行命令	凭证删除
3	AT+IIIDIDWRITE	执行命令	标识写入
4	AT+IIIDIDREAD	执行命令	标识读取
5	AT+IIIDIDDEL	执行命令	标识删除
6	AT+IIIDIDMODIFY	执行命令	标识修改
7	AT+IIIDSIGN	执行命令	身份签名
8	AT+IIIDVERIFY	执行命令	身份验签
9	AT+IIIDENCRYPT	执行命令	数据加密
10	AT+IIIDDECRYPT	执行命令	数据解密

AT命令格式示例如下。

1、凭证烧录

执行：

AT+IIIDADDCERT=type,cert,cert_len

返回：

<CR><LF>OK<CR><LF>

或

<CR><LF>ERROR<CR><LF>

参数：

type: 算法类型

0: RSA with PAD_PKCS1

1: SM2

cert：公钥值

cert_len ：公钥长度

2、凭证删除

执行：

AT+IIIDDELCCERT=type

返回：

<CR><LF>OK<CR><LF>

或

<CR><LF>ERROR<CR><LF>

参数：

type: 算法类型

0: RSA

1: SM2

3、标识写入

执行：

AT+IIIDIDWRITE=data,data_len

返回：

<CR><LF>OK<CR><LF>

或

<CR><LF>ERROR<CR><LF>

参数：

data：待写入的工业标识ID（经过加密）

data_len：待写入的工业标识ID的数据长度

4、标识读取

执行：

AT+IIIDIDREAD

返回：

<CR><LF>+ IIIDIDREAD:data, data_len<CR><LF>

<CR><LF>OK<CR><LF>

或

<CR><LF>ERROR<CR><LF>

参数：

data：工业标识ID

data_len：工业标识ID的数据长度

5、标识删除

执行：

AT+IIIDIDDEL

返回：

<CR><LF>OK<CR><LF>

或

<CR><LF>ERROR<CR><LF>

参数：/

6、标识修改

执行：

AT+IIIDIDMODIFY=data,data_len

返回：

<CR><LF>OK<CR><LF>

或

<CR><LF>ERROR<CR><LF>

参数：

data：待写入的工业标识ID（经过加密）

data_len：待写入的工业标识ID的数据长度

7、身份签名

执行：

AT+IIIDSIGN=data,data_len

返回：
<CR><LF>+IIIDSIGN:signed_data,signed_len<CR><LF>
<CR><LF>OK<CR><LF>
或
<CR><LF>ERROR<CR><LF>
参数：
data: 待签名的数据
data_len：待签名的长度
signed_data: 签名后的数据

8、身份验签

执行：
AT+IIIDVERIFY=data,data_len,signed_data,signed_data_len
返回：
<CR><LF>OK<CR><LF>
或
<CR><LF>ERROR<CR><LF>
参数：
data：未签名的内容
data_len：未签名内容的长度
signed_data：签名后的数据
signed_data_len：签名后数据的长度

9、数据加密

执行：
AT+IIIDENCRYPT=data,data_len
返回：
<CR><LF>+IIIDENCRYPT:encrypted_data,encrypted_data_len<CR><LF>
<CR><LF>OK<CR><LF>
或
<CR><LF>ERROR<CR><LF>
参数：
data：待加密的明文数据
data_len：待加密的明文数据长度
encrypted_data: 加密后的数据
encrypted_data_len: 加密后的数据长度

10、数据解密

执行：
AT+IIIDDECRYPT= encrypted_data, encrypted_data_len
返回：
<CR><LF>+IIIDDECRYPT:decrypted_data,decrypted_data_len<CR><LF>
<CR><LF>OK<CR><LF>
或
<CR><LF>ERROR<CR><LF>
参数：

encrypted_data:待解密的数据
encrypted_data_len：待解密的数据长度
decrypted_data: 解密后的数据
decrypted_data_len: 解密后的数据的长度