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/018-2021

工业互联网标识解析　主动标识载体 安全芯片技术要求

Industrial Internet identification resolution—Active identification carrier—Secure Element 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解析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： 中国移动通信集团有限公司

标准起草单位和主要起草人：

——中国移动通信集团有限公司：柳耀勇、习熹

——中国联合网络通信集团有限公司：贾雪琴、史可、黄蓉

——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、池程、尹子航、马宝罗、谢滨

——芯昇科技有限公司：肖青、孙东昱

——联通华盛通信有限公司:孙阳阳、韩梦梦

——联通华盛联通智慧安全科技有限公司:姚韬，蒋小燕

工业互联网标识解析 主动标识载体 安全芯片技术要求

1 范围

基于《工业互联网标识解析 主动标识载体 总体技术框架》，本文件规定了主动标识载体对安全芯片的基本能力要求、应用架构、应用要求。

本标准适用于工业互联网标识主动标识载体安全芯片的能力提供方等提供技术参考。

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。

《工业互联网标识解析 标识编码规范》

《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

下列术语和定义适用于本文件。

3.1

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）。

3.2

主动标识载体 active identifier carrier

承载工业互联网标识编码的载体，其自身具备主动建立广域通信连接的能力，或者是具备主动建立广域通信连接设备的内部组件。

3.3

芯片唯一编码 chip identifier

标识芯片唯一性的一串符号。

3.4

芯片信息预置 chip information initialization

主动标识载体在出厂阶段完成主动标识载体中芯片唯一编码及初始密钥的预置；

3.5

主动标识载体安全认证服务平台 security certification service of active identifier carrier

对主动标识载体中标识进行写入、读取、修改、删除等管理操作的平台。

3.6

缩略语

下列缩略语适用于本文件。

AID：应用标识（Application Identifier）

AES：高级加密标准，一种国际上常用的对称密钥加密算法

ECC：椭圆曲线加密算法，一种国际上常用的非对称密钥加密算法

RSA：一种国际上常用的非对称密钥加密算法

OTA：空中下载（Over The Air）

SDK：软件开发工具包（Software Development Kit）
SE：安全元件/安全芯片（Secure Element）
SHA256：一种国际上常用的密码杂凑算法
SIM：用户身份识别模块(Subscriber Identity Module)
TDES：三重数据加密标准，一种国际上常用的对称密钥加密算法
USIM：全球用户身份识别模块（Universal Subscriber Identify Module）

4 基于安全芯片的工业互联网主动标识载体的基本信息交互模型

基于安全芯片的工业互联网主动标识载体基本信息交互模型，参照《工业互联网标识解析 主动标识载体 总体技术框架》要求，针对安全芯片主动标识载体的交互逻辑、技术架构见图1所示。由安全芯片提供主动标识载体应用服务，并保障标识应用数据安全；主动标识载体SDK通过通用物理接口访问安全芯片标识应用，完成接口4标识操作指令控制，并与主动标识载体安全认证服务平台实现接口3标识管理的数据对接（主动标识载体SDK可根据实际场景需求，植入工业终端控制器MCU或蜂窝通信模组内，通过接口4与安全芯片交互）；工业终端APP或控制器MCU通过接口5操作指令，访问主动标识载体SDK，完成标识管理及标识解析应用业务。

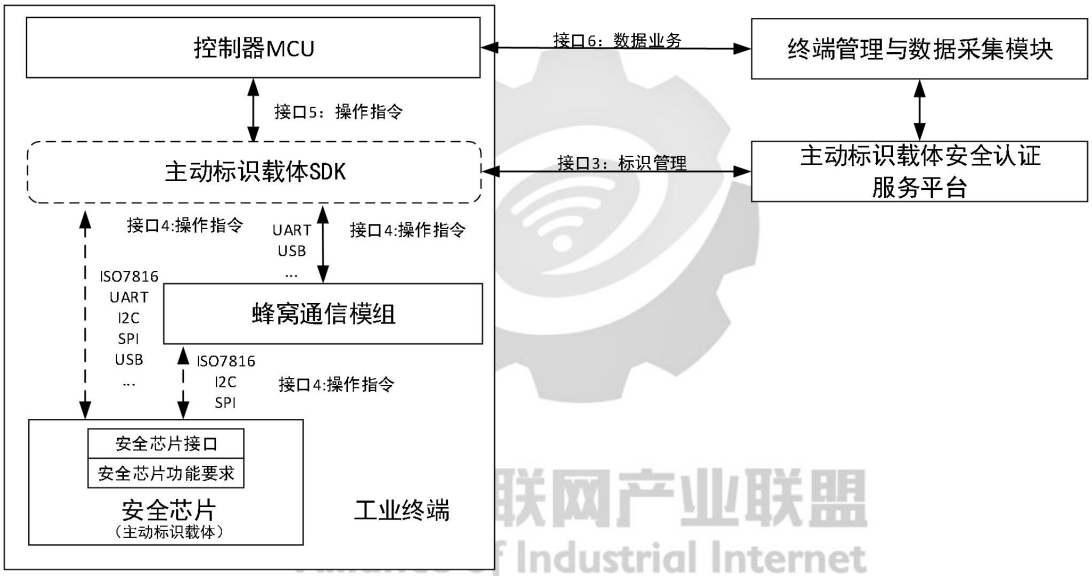


图1 主动标识载体-安全芯片信息交互图

5 主动标识载体 安全芯片 SDK 要求

主动标识载体安全芯片通过SDK对接主动标识载体安全认证服务平台，将平台下发的标识管理操作指令（包括下发标识凭证、增删改查工业互联网标识、企业接口/载体服务平台URL等），转换为安全芯片终端接口指令格式，对载体内标识进行信息维护及管理。同时为工业终端提供基于标识的数据推送及获取安全通道接口能力。主动标识载体SDK可通过通信模组桥接到安全芯片，也可以直连到安全芯片。通过桥接方式连接，安全芯片既可以承载工业互联网标识应用，也可以承载SIM/USIM应用。

安全芯片SDK的功能包括：

(1) 服务工业终端应用，进行业务能力承接，实现基于标识的数据推送及获取安全通道接口；

(2) 服务主动标识载体安全认证服务平台，进行安全芯片和主动标识载体安全认证服务平台模块之间报文转发，实现标识管理及信息更新；

(3) 安全芯片通讯管理,比如接口驱动，接口事务等；

6 主动标识载体 安全芯片应用架构

安全芯片应用采用分层设计，主动标识载体安全芯片应用架构见图2:

（1）硬件及驱动层：提供硬件和驱动支持；

（2）内核层：负责系统任务调度、空间管理、安全管理、通信管理等功能，为应用层提供支持；

（3）应用层：负责应用逻辑的实现，可以有工业互联网标识应用及其他应用；

（4）数据：每个应用的数据隔离，存储在各自的数据空间中，仅自身可以访问，工业互联网标识应用的数据包括主动标识、主动标识对应的密钥，及其他数据；

（5）工业互联网标识应用：负责工业互联网标识的写入、删除、修改、查询等功能；

（6）其他应用：业务所需的其他应用，如SIM应用、USIM应用、其他安全应用等。

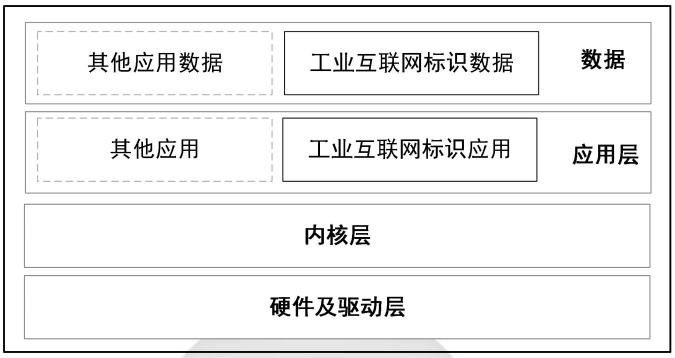


图2 安全芯片应用架构图

7 主动标识载体 安全芯片基本能力要求

7.1 安全芯片整体要求

安全芯片具备独立安全内核，专用密码算法硬件计算单元，独立安全存储空间，地址加扰，加密存储，访问控制，硬件真随机数，能够抗实验室级软件攻击及物理攻击。

7.2 安全芯片算法要求

安全芯片应支持多种加密算法，适用于多种工业互联网标识解析应用场合。安全芯片推荐采用国家密码管理机构核准的密码算法，建议支持国密标准SM2、SM3、SM4以及SM9算法的一种或几种。

对称算法应至少支持SM4、AES、TDES中的一种。

非对称算法应至少支持SM2、SM9、ECC、RSA中的一种。

杂凑算法应至少支持SM3、SHA256中的一种。

7.3 安全认证要求

安全芯片应通过EAL4+或EAL4+以上认证。

安全芯片应通过国家商用密码产品二级认证；

7.4 接口要求

安全芯片应提供通用物理传输接口供工业终端进行安全数据交互，接口不限于ISO7816,SPI,I2C。

8 主动标识载体 安全芯片应用要求

8.1 安全芯片应用加载要求

工业互联网标识应用可在出厂时预制在安全芯片中，也可以通过OTA方式下载。

8.2 载体标识要求

安全芯片支持载体唯一标识存储，并防止被恶意篡改。

8.3 密钥要求

安全芯片中应包含多种功能密钥，用于不同场景的安全加固，主动标识载体安全芯片密钥结构见图3。

初始的功能密钥应在安全芯片初始化阶段完成预制。

主动标识载体安全芯片中应包含载体容器及标识容器，其中载体容器包含载体信息及载体密钥(总体技术要求中的载体密钥M0,初始凭证C0)，用于识别载体唯一身份，并用于标识管理过程的安全加固；标识容器中包含工业互联网标识及标识密钥(总体技术要求中的标识服务平台凭证C1),用于标识的身份识别，并用于标识应用过程的安全加固。

支持的功能密钥类型至少包括：

（1）载体管理-加密密钥

载体管理-加密密钥用于对载体标识及信息维护过程（对应总体技术-接口3）中进行安全加密，防止信息泄露；

（2）载体管理-认证密钥

载体管理-认证密钥用于认证载体标识及信息维护过程（对应总体技术-接口3）来自合法的标识载体，防止信息篡改或伪造；

（3）载体管理-平台认证密钥

载体管理-平台认证密钥用于认证载体管理平台/主动标识载体安全认证服务平台下发的标识管理报文（对应总体技术-接口3），识别平台合法身份，并防止信息篡改及伪造；

（4）标识业务-加密密钥

标识业务-加密密钥用于对标识业务数据（对应总体技术-接口6）进行安全加密，防止信息泄露；

（5）标识业务-认证密钥

标识业务-认证密钥用于生成工业终端上行标识业务的认证信息（对应总体技术-接口6），终端采集模块可通过认证信息的正确性来识别合法的工业终端及标识；

（6）标识服务平台-认证密钥

标识服务平台-认证密钥用于确认平台下发的标识业务数据来自合法的标识服务平台（对应总体技术-接口6），防止信息篡改或伪造；

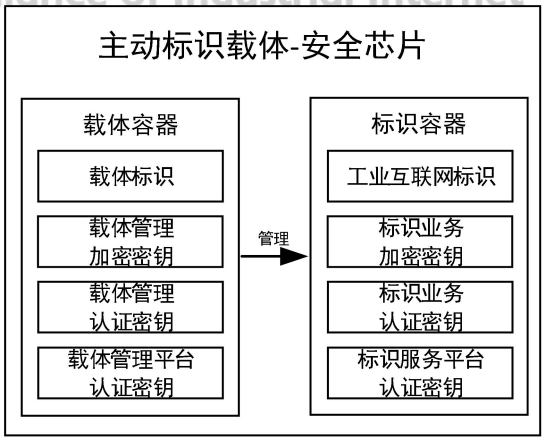


图3 安全芯片密钥结构

8.4 安全芯片初始化

安全芯片在出厂阶段应完成初始化，包括加载固件、载体管理保护密钥、载体管理认证密钥；

初始化时应增加给安全芯片设置唯一设备可信标识，载体标识一旦写入不可修改。

8.5 标识存储要求

主动标识载体应至少支持1组255字节标识存储能力；

主动标识载体应支持标识服务平台URL、企业节点URL等信息存储；

为扩展主动标识载体的应用场景，提升主动标识载体的标识管理能力，主动标识载体宜支持多组标识空间，实现对工业终端下的多组从设备提供标识管理服务。

8.6 敏感数据保护

安全芯片内存储的标识、载体管理密钥、标识密钥、标识服务平台/企业平台URL等信息应保证存储安全，在信息传输过程中应保障不被非法篡改，针对密钥等关键敏感操作应保障在数据传输过程不被非法窃听。

8.7 安全机制要求

针对标识管理操作（增、删、改、查）对标识及标识相关信息的修改应采用载体管理认证密钥(或主动标识载体安全认证服务平台公钥)校核操作指令来着合法的载体服务平台；标识及标识信息修改的操作指令应采用载体管理保护密钥加密保护；

标识业务交互过程中宜采用标识业务安全保护密钥对标识业务数据进行加密保护，应采用标识业务认证密钥计算消息认证信息；

标识管理操作及标识业务交互过程中应设计防重放因子，一方面，生成的报文不会重复。另一方面能够识别并过滤掉重放的报文，有效避免重放攻击；

标识管理操作及标识业务交互过程中宜添加随机数，提升不可预测性；

8.8 功能要求

安全芯片应满足《工业互联网标识解析 主动标识载体 总体技术框架》规范要求的标识管理能力，实现对标识及标识信息的增加、删除、修改、查询，具体的指令细节可参考附录A。

安全芯片应支持载体管理密钥、标识密钥的管理能力，主动标识载体安全芯片功能见图4。

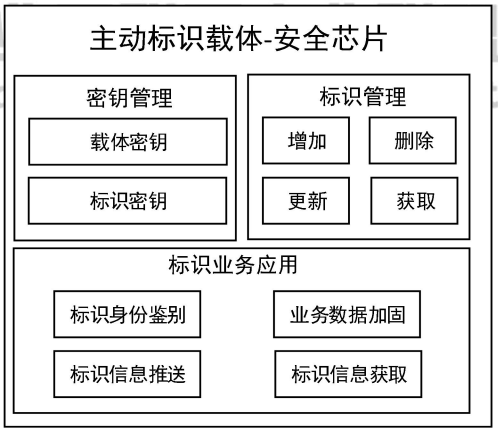


图4 主动标识载体 安全芯片功能框图

安全芯片应提供基于工业互联网标识、标识密钥的可信标识应用服务，保护标识业务可信安全，具体的功能如下：

（1）工业互联网标识身份识别：安全芯片应提供基于标识业务认证密钥生成标识身份认证数据，实现标识应用过程的唯一身份识别；

（2）工业互联网标识信息推送：安全芯片应提供工业终端向主动标识载体安全认证服务平台/企业节点推送标识信息的服务能力，并使用标识业务密钥实现信息交互的安全加固；

（3）工业互联网标识信息获取：安全芯片应提供接口，接收主动标识载体安全认证服务平台/企业节点下发的标识业务数据，使用标识业务密钥验证数据真实性，并向工业终端返回；

（4）工业终端的数据安全加固：安全芯片宜提供可信的链路加密通道能力，实现工业终端与数据采集模块之间的业务数据的安全加固，防止业务数据泄露及篡改。

其中工业互联网可信标识应用服务基本应用示例见本文件的资料性附录B。

附 录 A

（资料性附录）

主动标识载体安全芯片 APDU 指令说明

A.1 指令结构

安全芯片仅支持特定结构的指令。这些指令由终端通过以上接口发送到安全芯片。指令结构符合APDU协议。指令分为命令和响应两种结构，具体如下：

命令结构：

字段	长度	说明
CLA	1	指令类型
INS	1	指令名称
P1	1	参数1
P2	1	参数2
Lc	0/1	命令数据长度
Data	var	命令数据
Le	0/1	响应数据长度

响应结构：

字段	长度	说明
Data	var	响应数据
SW1	1	状态字1
SW2	1	状态字2

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	85	执行条件不满足
69	82	安全状态不满足
6A	80	数据域参数错误
6A	82	找不到文件
6A	86	P1或P2参数错
6A	88	找不到数据
67	00	Lc长度错误

A.2 接口指令集

接口指令集如下：

序号	指令名称	说明
1	Identifier Request	申请工业互联网标识
2	Identifier Management	管理工业互联网标识（增/删/改）

3	Identifier Upload	标识上行数据业务
4	Identifier Parse	标识下行数据业务
5	Identifier Read	读取工业互联网唯一标识
6	GetSN	获取安全芯片载体唯一序列号
7	Identifier Info Read	读取工业互联网标识附加信息

A.3 申请工业互联网标识 Identifier Request

定义与范围：该指令用于在应用阶段生成向主动标识载体安全认证服务平台申请标识报文；申请报文中携带主动标识载体唯一序列号、防重放因子及载体合法身份认证信息等，并支持用户输入标识申请的附加注册信息；

指令报文编码如下：

字段	值(Hex)	说明
CLA	XX	
INS	E1	申请工业互联网标识
P1	00	
P2	XX	报文安全模式
Lc	var	数据域长度
Data	‘XXXX’	标识注册附加信息
Le	XX	

指令数据：

字段	长度	说明
Info	XX	标识注册附加信息

响应数据：

字段	长度	说明
SN	8	芯片SN
SecurityMode	1	报文安全模式
Operation	1	标识管理业务操作码-0x70
Random	8	随机数
Info	XX	附加信息明文/明文
MAC	4/64	以上数据的MAC/签名

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	82	安全错误
69	85	执行条件不满足
6A	80	数据域参数错误
6A	81	功能不支持

6A	86	P1或P2参数错
6A	88	找不到数据
67	00	Lc长度错误

A.4 **标识管理处理** Identifier Management

定义与范围：该指令用于解析主动标识载体安全认证服务平台下发的标识管理处理报文，实现对标识及标识信息的增、删、改。执行指令将首先验证报文是否具备主动标识载体安全认证服务平台的合法身份信息，并对防重放因子进行校验，并采用载体管理加密密钥解密标识管理报文，获取工业互联网标识及凭证信息；

指令报文编码如下：

字段	值(Hex)	说明
CLA	XX	
INS	E3	标识管理处理
P1	00	
P2	00	
Lc	XX	管理报文长度
Data	XX	
Le	无	

指令数据：

字段	长度	说明
SecurityMode	1	报文安全模式
Operation	1	标识管理业务操作码 F0-标识写入 F1-标识修改 F2-标识删除 F3-无操作
Random	8	随机数
Manage ciphertext	Var	标识管理报文密文（其中包含防重放因子、标识、凭证、企业节点URL等信息）
MAC	4/64	以上数据的MAC/签名数据

响应数据：

无

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	85	执行条件不满足
6A	81	功能不支持

6A	86	P1或P2参数错
6A	88	找不到数据

A.5 **标识上行业务数据** Identifier Upload

定义与范围：该指令用于在标识应用阶段，利用标识及标识凭证信息对其标识信息及应用数据业务进行安全加固，生成标识的合法身份认证信息，企业节点或主动标识载体安全认证服务平台可实现对数据业务的身份识别；

指令报文编码如下：

字段	值(Hex)	说明
CLA	XX	
INS	E5	标识上行业务数据
P1	00	
P2	XX	安全模式
Lc	var	待保护的业务数据长度
Data	‘XXXX’	待保护的业务数据
Le	00	

指令数据：

字段	长度	说明
Index	2	标识索引
Data	XX	标识业务数据

响应数据：

字段	长度	说明
Index	2	标识索引
SecurityMode	1	安全模式
Operation	1	标识业务操作码 – 60
Random	8	随机数
Data	xx	标识业务数据明文/密文
MAC	4/64	标识身份认证MAC或签名

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	82	安全错误
69	85	执行条件不满足
6A	80	数据域参数错误
6A	81	功能不支持
6A	86	P1或P2参数错

6A	88	找不到数据
67	00	Lc长度错误

A.6 标识下行业务数据 Identifier Parse

定义与范围：该指令用于在标识应用阶段，实现对企业节点下发标识业务数据进行认证及解析， 执行指令将首先验证报文是否具备标识认证平台的合法身份信息，并对防重放因子进行校验，并采用标识业务加密密钥解密标识业务报文，将解密后的业务数据返回至安全芯片SDK/工业终端；

指令报文编码如下：

字段	值(Hex)	说明
CLA	XX	
INS	E7	标识下行业务数据
P1	00	
P2	00	
Lc	var	平台下行的标识业务数据长度
Data	‘XXXX’	平台下行的标识业务数据
Le	00	

指令数据：

字段	长度	说明
Index	2	标识索引
SecurityMode	1	安全模式
Operation	1	标识业务操作码 - E0
Random	8	随机数
Data	xx	标识业务数据明文/密文
MAC	4/64	标识认证平台身份认证MAC或签名

响应数据：

字段	长度	说明
Data	XX	标识业务数据明文

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	82	安全错误
69	85	执行条件不满足
6A	80	数据域参数错误
6A	81	功能不支持
6A	86	P1或P2参数错
6A	88	找不到数据
67	00	Lc长度错误

A.7 读取标识载体唯一序列号 GetSN

定义与范围：该指令用于获取主动标识载体的唯一标识，用于载体的身份识别。
指令报文编码如下：

字段	值(Hex)	说明
CLA	XX	
INS	A8	获取载体序列号
P1	00	
P2	00	
Lc	不存在	
Data	不存在	
Le	08	

指令数据：

无

响应数据：

字段	长度	说明
SN	8	载体唯一标识

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	82	安全错误
69	85	执行条件不满足
6A	80	数据域参数错误
6A	81	功能不支持
6A	86	P1或P2参数错
6A	88	找不到数据
67	00	Lc长度错误

A.8 读取工业互联网标识 Identifier Read

定义与范围：该指令用于获取主动标识载体内存储的工业互联网标识；
指令报文编码如下：

字段	值(Hex)	说明
CLA	XX	
INS	EA	获取工业互联网标识
P1	Xx	标识索引
P2	00	
Lc	不存在	
Data	不存在	

Le	xx	

指令数据：

无

响应数据：

字段	长度	说明
Identifier	XX	工业互联网标识

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	82	安全错误
69	85	执行条件不满足
6A	80	数据域参数错误
6A	81	功能不支持
6A	86	P1或P2参数错
6A	88	找不到数据
67	00	Lc长度错误

A.9 读取工业互联网标识相关信息 Identifier Info Read

定义与范围：该指令用于获取主动标识载体内存储的其他相关信息，例如主动标识载体认证服务平台URL,企业节点URL等；

指令报文编码如下：

字段	值(Hex)	说明
CLA	XX	
INS	EC	获取工业互联网标识相关信息
P1	XX	标识索引
P2	XX	信息类别
Lc	不存在	
Data	不存在	
Le	xx	

指令数据：

无

响应数据：

字段	长度	说明
Info	XX	工业互联网标识相关信息

状态字定义：

SW1	SW2	含义
90	00	执行成功
69	82	安全错误
69	85	执行条件不满足
6A	80	数据域参数错误
6A	81	功能不支持
6A	86	P1或P2参数错
6A	88	找不到数据
67	00	Lc长度错误

附　录 B

（资料性附录）

主动标识载体 安全芯片-可信标识业务示例应用

B.1 业务描述

智能表计是智慧城市的典型应用，水、气、电表广泛应用于城市居民生活。智慧燃气表作为能源计量的典型设备广泛分布在千家万户中，针对能源的计量、检定、安全、管理等问题成为各燃气运营公司及监管单位的重点工作；通常情况下，智慧燃气表直接与燃气公司运营系统对接，并由运营系统与政府平台、监管单位等系统对接；

B.2 主动标识载体 安全芯片在智慧燃气的可信标识业务的应用方案

为提升智慧燃气表的管理效率及数据可靠性，围绕燃气表标识，通过主动标识服务平台向燃气表标识解析信息，提供目标服务平台的链接信息。

燃气表依据安全芯片返回的标识业务数据，向目标服务平台推送个性化服务数据，智慧燃气应用架构见图 B.1，具体流程描述如下：

B.2.1 前置条件

智慧燃气表集成安全芯片主动标识载体；

智慧燃气表完成标识注册，并通过主动标识载体安全认证服务平台将工业互联网标识及密钥的写入安全芯片中；

政府监管服务平台在主动标识载体安全认证服务平台完成注册、并获取目标智慧燃气表标识的访问权限；

B.2.2 基本应用

（1）政府监管服务平台修改指定目标燃气表工业互联网标识的标识信息，在目标服务连接信息字段中添加监管平台的URL，标记燃气表进入检定模式；

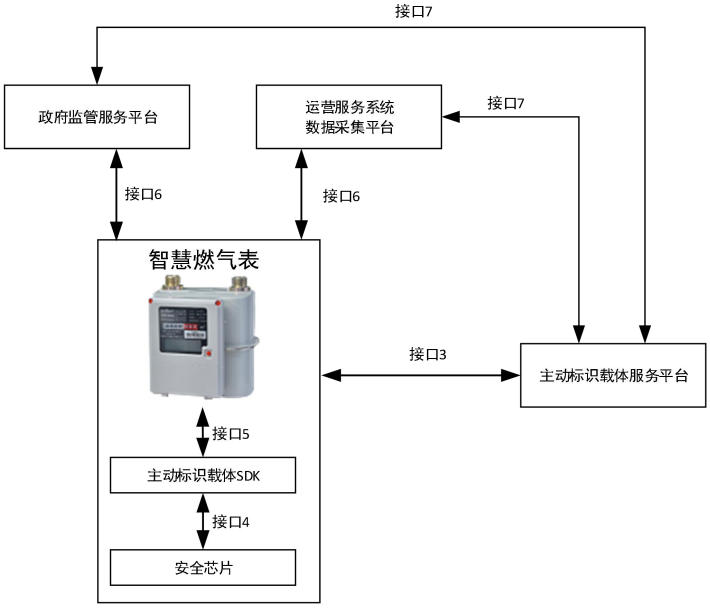
（2）智慧燃气表通过安全芯片生成标识业务数据推送请求，并向主动标识载体安全认证服务平台推送；

（3）主动标识载体安全认证服务平台通过标识业务密钥验证标识业务数据合法性，并通过燃气表标识解析标识信息，其中包含监管平台添加的URL；

（4）主动标识载体安全认证服务平台将标识解析信息通过标识业务密钥加固后推送至智慧燃气表；

（5）智慧燃气表请求安全芯片认证解密标识平台发送的标识业务数据；

（6）智慧燃气表通过标识业务数据中携带的标识解析数据，获取监管服务平台的URL，并与目标平台建立连接，推送燃气计量数据。



图B.1 智慧燃气应用架构图

B.3 主动标识载体 安全芯片在智慧燃气的数据安全应用方案

安全芯片主动标识载体依托安全运行环境，不仅存储工业互联网标识，还承载标识业务密钥实现标识身份认证及标识业务数据安全加固；同样智慧燃气业务亦可采用标识业务密钥系统实现业务层的数据安全加固，提升业务数据安全等级；具体流程描述如下：

B.3.1 前置条件

智慧燃气表集成安全芯片主动标识载体。

智慧燃气表完成标识注册，并通过主动标识载体安全认证服务平台将工业互联网标识及密钥的写入安全芯片中。

B.3.2 基本应用

（1）智慧燃气表组装业务数据报文，请求安全芯片使用标识业务密钥对业务数据进行加密和认证；

（2）智慧燃气表将加固后的业务数据报文及工业互联网标识推送至数据采集平台；

（3）数据采集平台收到智慧燃气表发送的业务数据后，请求主动标识载体安全认证服务平台对业务数据进行身份认证，确认数据来自合法的智慧燃气表；并将业务数据解密后返回至数据采集平台；

（4）数据采集平台获取认证解密后的业务数据，执行运营管理业务处理；

参考文献

[1] GB/T 32918.1-2016 SM2椭圆曲线公钥密码算法 第1部分：总则

[2] GB/T 32918.2-2016 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

[3] GB/T 32918.3-2016 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

[4] GB/T 32918.4-2016 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

[5] GB/T 32905-2016 SM3密码杂凑算法

[6] GB/T 32907-2016 SM4分组密码算法