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/019-2021

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

Identification and resolution of industrial internet—Active identification carrier—UICC Card 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： 联通华盛通信有限公司

标准起草单位和主要起草人：

——联通华盛通信有限公司：孙阳阳、韩梦梦、曹龙涛

——中国联合网络通信有限公司：贾雪琴、史可，黄蓉

——中国信息通信研究院：刘澍、田娟、尹子航

——联通智慧安全科技有限公司：姚韬

——中移物联网有限公司：柳耀勇、习熹、肖青

——芯昇科技有限公司：孙东昱、刘勇

——紫光国芯微电子股份有限公司：霍航宇

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

1 范围

本文件规定通用集成电路卡作为工业互联网标识解析主动标识载体的技术架构、基本功能要求、工业应用要求等内容。

本规范适用于为移动通信终端中的工业互联网标识解析主动标识载体通用集成电路卡提供技术参考。为使用主动标识载体通用集成电路卡的行业用户提供技术参考。

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。

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

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

标识解析 Identifier resolution

根据标识编码查询目标对象网络位置或者相关信息。

3.3 缩略语

下列缩略语适用于本文件。

ARF 访问控制文件 Access Rule Files

ARA-M 主访问控制应用 Access Rule Application Master

AID 应用程序标识符 Application Identifier

UICC 通用集成电路卡 Universal Integrated Circuit Card

4 主动标识载体 通用集成电路卡技术架构

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所示，主要描述主动标识载体、工业终端（含主动标识载体SDK）、主动标识载体管理模块、主动标识载体服务平台、终端管理与数据采集模块、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。

本规范针主动标识载体模块对主动标识载体通用集成电路卡（UICC）的基本能力要求、应用要求进行规定。

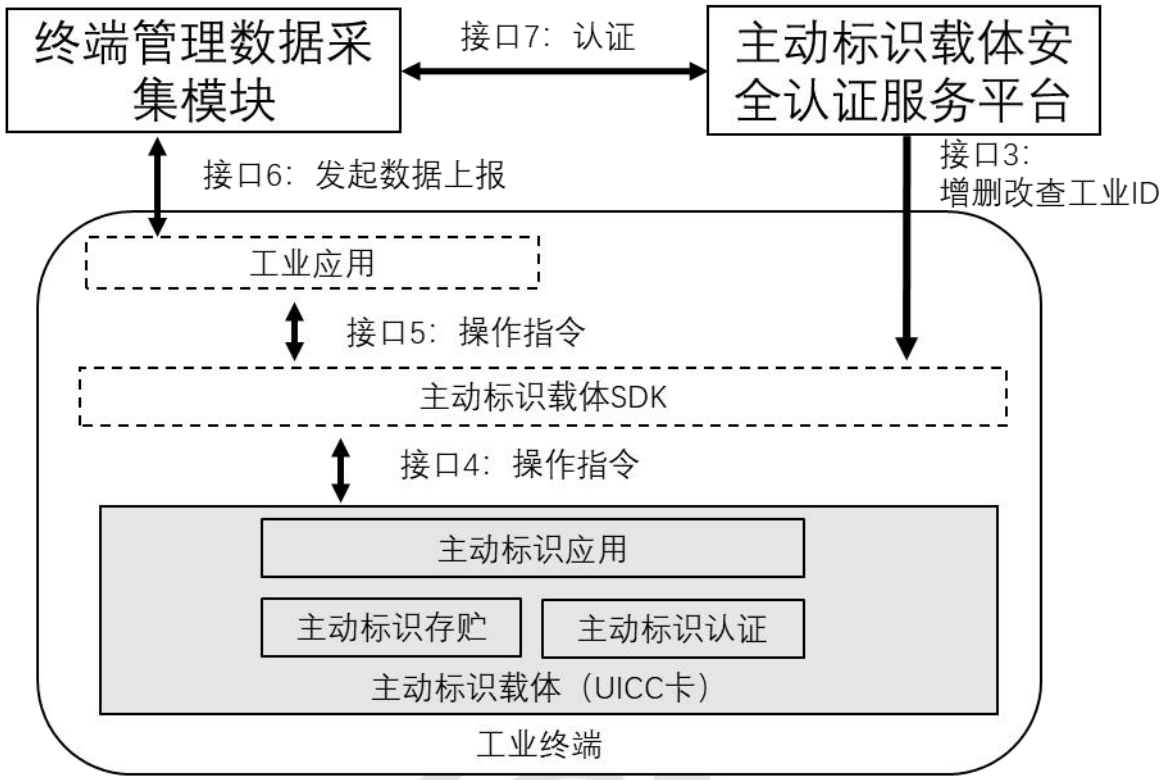

图1 主动标识载体在主动标识载体总体技术架构中的定位

注：工业ID 是工业互联网标识的简称。

主动标识载体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；支持根据主动标识载体服务平台的请求写入、删除、修改、查询、存储工业互联网标识；支持主动标识载体服务平台的身份验证流程；支持载体本地安全存储。与主动标识载体SDK对接，支持工业标识得写入，删除，修改等指令。（接口4）

5 主动标识载体 通用集成电路卡基本能力要求

UICC卡片内部结构基本分4层：物理平台层，操作系统层，安全域层，应用层，主动标识载体在以上4层结构中的基本能力要求见图2。

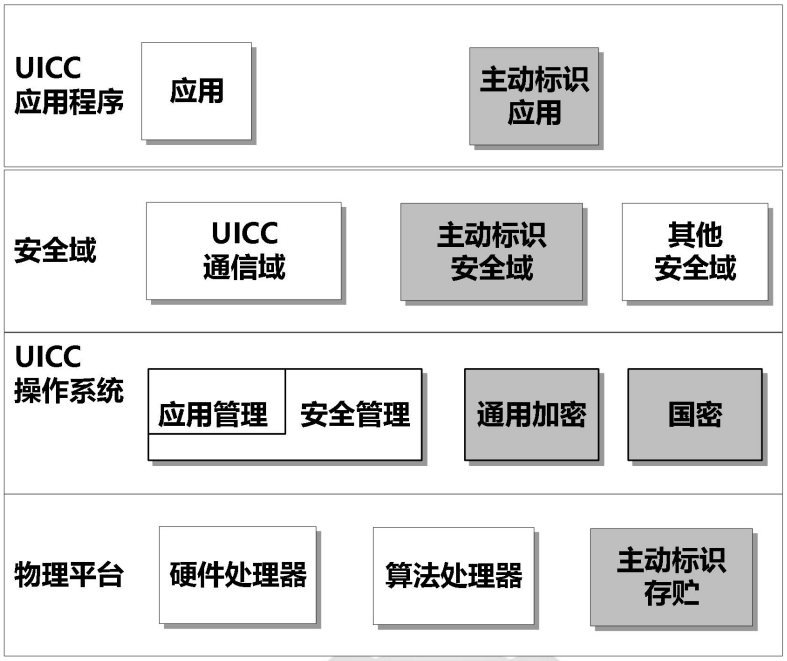

图2 主动标识载体通用集成电路卡内部结构

- 物理平台：硬件处理器，算法寄存器，物理存储。
- UICC操作系统：管理UICC卡硬件物理平台，管理UICC卡片安全域名，管理UICC应用。
- 安全域：为应用提供安全保护，通讯协议等，不同安全域互相隔离。
- UICC应用程序：根据业务要求，提供相应得接口指令。

5.1 存储要求

UICC卡创建私有文件保存工业互联网标识，工业互联网标识文件不允许直接访问，只能通过特定接口函数进行访问。

5.2 安全算法要求

UICC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。UICC卡宜采用国家密码管理机构核准的密码算法，采用国密标准SM2、SM3、SM4以及SM9算法的一种或几种。支持具有实现安全存储、数据加/解密、身份认证等安全控制功能。

对称算法应至少支持SM4、AES、DES、TDES中的一种；

非对称算法应至少支持SM2、ECC、RSA中的一种；

杂凑算法应至少支持SM3、SHA256中的一种。

5.3 应用安全域及接口协议要求

扩展应用需要独立的安全管理和数据管理，扩展应用和其他应用需要进行逻辑防火墙进行隔离，各扩展安全域中的应用，不允许跨安全域互相访问。

UICC应提供通用物理传输接口，供工业互联网终端进行安全数据交互，接口不限于ISO 7816。

6 主动标识载体 通用集成电路卡应用要求

根据卡片能力，UICC 可分为A型（高性能安全卡片）和B型（低性能安全卡）。其中，A型 UICC 支持国密算法和证书验证算法。B型UICC仅支持基本对称加密算法和非对称算法。

6.1 A 型通用集成电路卡要求

6.1.1 应用要求

UICC 创建私有文件，应包括：证书状态文件、卡片私钥、卡片证书、IMEI(多个 IMEI 值)、服务器公钥、PIN、工业 ID 文件（多条记录长度 64 字节可存储 64 个英文字符或 128 个十六进制数字）。

6.1.2 安全域扩展业务卡片预置条件

（1） UICC公私密钥对：密钥对由卡商生成、预制，公钥需要提交给管理平台。

（2） 初始PIN：初始为固定值，允许进行修改。

（3） 安全管理平台公钥：由安全服平台管理系统生成公私密钥对，私钥保存在平台加密机中，公钥由安全管理平台管理，并需要把此公钥预制到UICC上，用来校验安全管理平台身份。

6.1.3 UICC 身份凭证申请

（1） 完成申请下载安装证书;

（2） UICC证书已经卡片需要的公私密钥可以采用预制的方式存入到UICC卡片中，也可以采用用户下载的方式。

6.1.4 写入工业互联网标识

工业互联网标识是通过主动标识载体安全认证服务平台使用安全的方式写入到标识载体中,写入流程见图3。

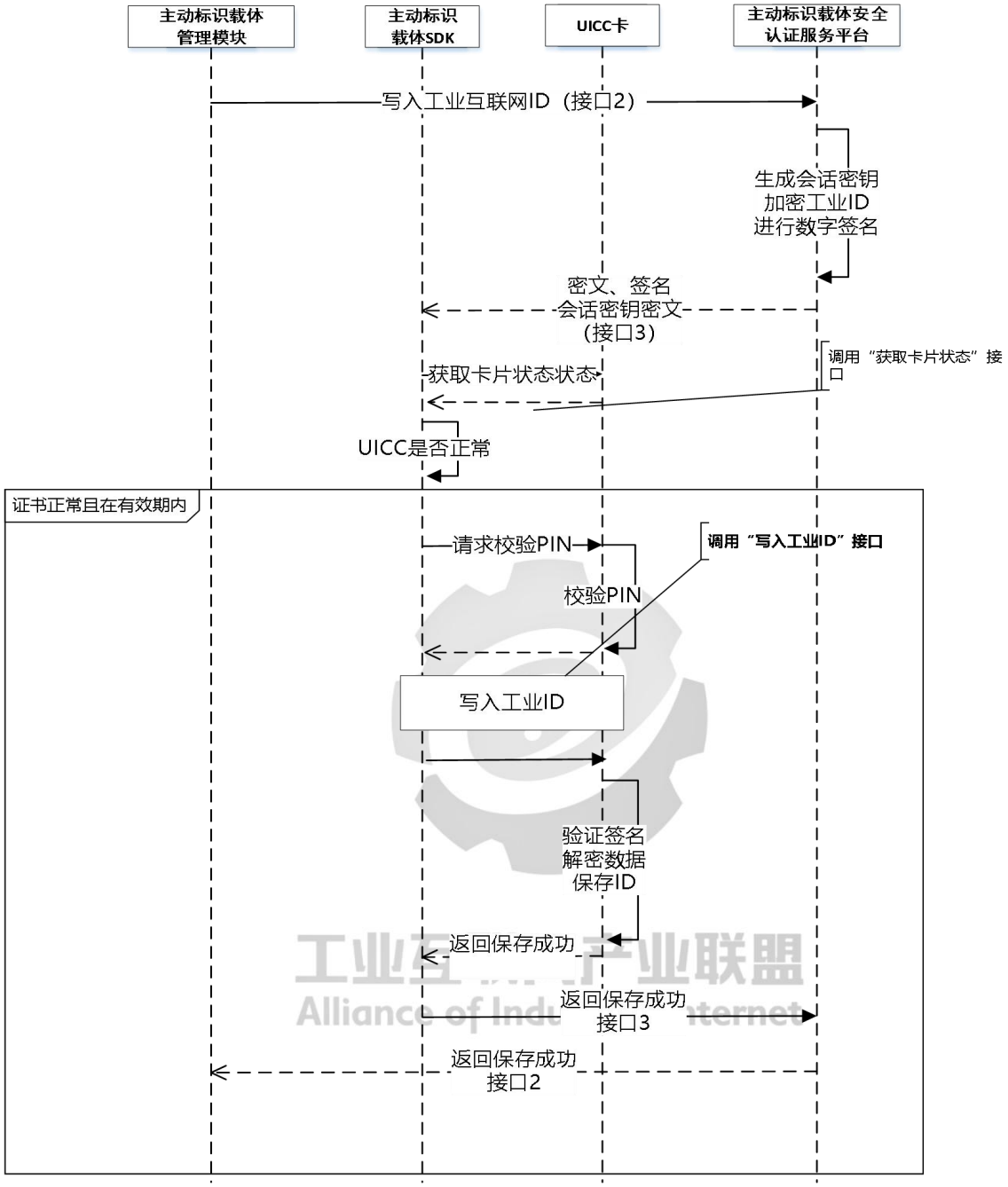

图3 主动互联网标识写入流程

注：工业ID 是工业互联网标识的简称。

（1） 主动标识载体管理模块将工业ID，标识载体唯一标识（ICCID，MSISDN等）信息发送为主动标识载体安全认证平台。参见总体框架（接口2）

（2） 主动标识载体安全认证服务平台生成会话密钥，使用会话密钥对工业ID进行加密和数据签名，采用安全的协议发送给主动标识载体SDK。

（3） 主动标识载体SDK检查UICC卡片状态是否正常，如果状态正常继续执行流程。

（4） 主动标识载体SDK根据预制（或企业修改）pin，进行本地安全校验平校，校验通过后继续执行流程。

（5） 主动标识载体SDK执行“写入工业ID”指令，将主动标识载体安全认证服务平台下发的安全数据发送给UICC卡。

（6） UICC卡验证数据签名，验证成功过，根据数据生成过程密钥，对数据进行解密，将工业ID原文保存到本地。保存成功后通知主动标识载体SDK。

（7） 主动标识载体SDK将写入成功信息发送给主动标识载体安全认证服务平台，平台保存相关记录

（8） 主动标识载体安全认证服务平台写入成功信息发送给主动标识载体管理模块。

6.1.5 标识读取

主动标识载体管理模块通过主动标识SDK对工业互联网标识进行读取，流程见图4。

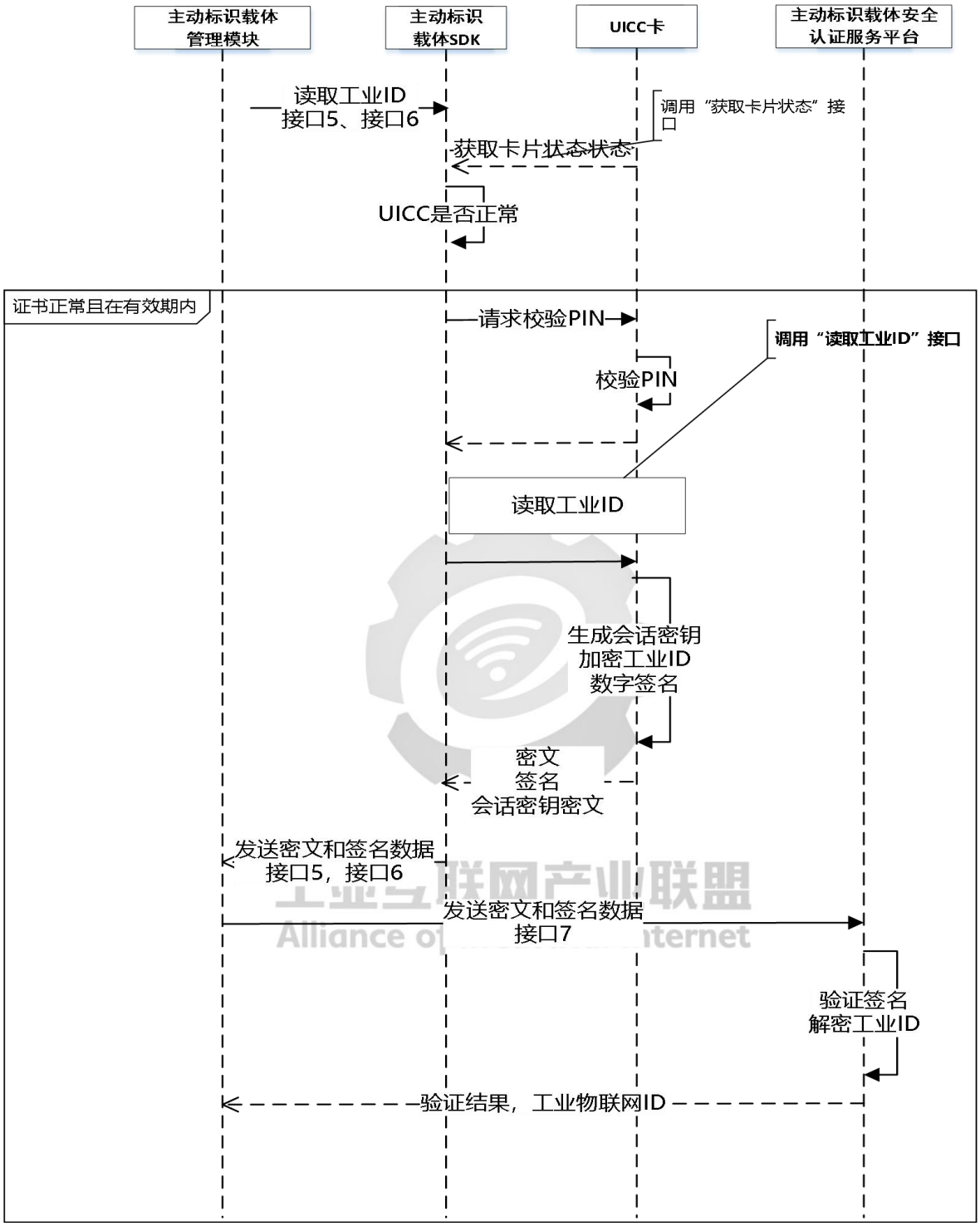

图4 工业互联网标识读取流程

（1） 主动标识载体管理模块通过工业应用app向主动标识载体SDK发起读取工业ID的请求，或者工业应用主动发起读取工业ID的请求，接口5、接口6。

（2） 主动标识载体SDK检查UICC卡片状态是否正常，如果状态正常继续执行流程。

（3） 主动标识载体SDK根据预制（或企业修改）pin，进行本地安全校验平校，校验通过后继续执行流程。

（4） 主动标识载体SDK执行“读取工业ID”指令，接口4。
（5） UICC卡生成过程密钥，对工业ID进行加密并对数据进行数字签名。将结果数据返回给主动标识载体SDK
（6） 主动标识载体SDK将收到的数据发送给主动标识载体管理模块，接口5、接口6。
（7） 主动标识载体管理模块根据需要将密文数据和签名发送给主动标识载体安全认证平台
（8） 主动标识载体安全认证平台对数据进行验签和解密，将验签结果和工业ID名为发送给主动标识载体管理模块

6.1.6 删除工业互联网标识

删除工业互联网标识流程与本规范6.1.4写入工业互联网标识流程一致，写入特定数据作为删除的标记，代表删除记录。

6.1.7 PIN 码修改（可选）

pin作为本地安全访问口令，发行时预制统一值，工业企业使用主动载体时，可使用接口5和接口4提供的接口指令进行数值修改。Pin码修改的流程见图5。

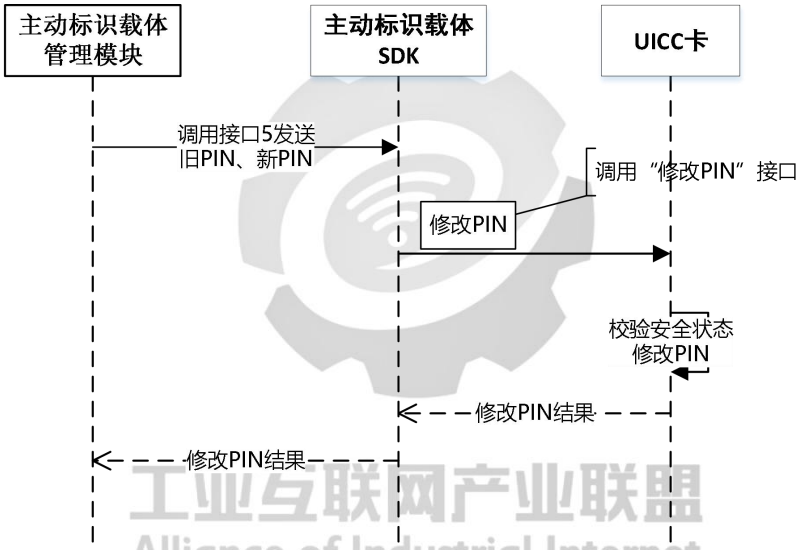

图5 PIN码修改流程

（1） 主动标识载体管理模块直接或通过工业应用APP调用主动标识载体SDK接口，出入旧pin和新pin的数据。接口5
（2） 主动标识载体SDK使用指令将数据传入UICC卡。接口4
（3） UICC卡校验旧pin，如成功则用新pin数据更新pin。
（4） UICC将修改pin结果通知主动标识载体SDK
（5） 主动标识载体SDK将修改pin结果通知主动标识载体管理模块。

6.1.8 通用集成电路卡应用接口指令

UICC卡片接口（接口4），应符合卡片基本通讯指令符合ISO/IEC 7816要求。具体命令列表见表1。

表 1 UICC 卡接口函数表

序号	指令名称	中文名称	说明
1	getSimKeyStatus	获取卡片状态	获取 UICC 卡 ICCID、版本号、证书状态和是否激活

2	getRandom	获取随机数	获取随机数
3	UICCsignature	卡签名	使用卡私钥对 ICCID 和随机数进行签名
4	getCSR	生成 CSR	生成用于申请UICC 卡证书的CSR 文件
5	saveCertificate	保存证书	保存证书
6	bindSIMKEY	保存绑定关系	保存绑定关系
7	verifyPIN	校验 PIN	验证 UICC 卡的 PIN 值
8	modifyPIN	修改 PIN	修改 UICC 卡的 PIN 值（可选）
9	resetPIN	重置 PIN	重置 UICC 卡的 PIN 值（可选）
10	writeID	写入工业 ID	写入工业互联网标识
11	readID	读取工业 ID	读取工业互联网标识

具体的指令细节参见附录A

6.2 B 型通用集成电路卡要求

UICC卡应支持的标识管理能力，实现对标识及标识信息的增加、删除、修改、查询；

UICC卡应支持载体管理密钥、标识密钥的管理能力；

UICC卡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） 应具备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的能力；UICC卡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） 应能根据主动标识载体服务平台的请求写入、读取、存储工业互联网标识；

（3） 应支持主动标识载体服务平台的身份验证流程；UICC卡应提供接口，接收主动标识载体服务平台/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。

具体命令列表见表2。

表 2 UICC 卡接口函数表

序号	指令名称	中文名称	说明
1	GET RAND	获取随机数	获取随机数
2	IMPORT KEY	导入密钥	导入密钥
3	READ IDENTIFIER	读取标识	读取工业互联网标识
4	WRITE IDENTIFIER	写入标识	写入工业互联网标识
5	DELETE IDENTIFIER	删除标识	删除工业互联网标识

具体的指令细节参见附录B。

附　录 A

（规范性附录）

A 型（高性能）通用集成电路卡片指令集

A.1 命令结构体格式

Command Message：

Code	**Length**	**Meaning**
CLA	1	Calss
INS	1	Instruction
P1	1	Parameter 1
P2	1	Parameter 2
Lc	0/1	Length of data field
Data	var	The data field
Le	0/1	Length of Response

Response Message:

Code	**Length**	**Meaning**
Data	var	命令响应数据
SW1	1	Status word 1
SW2	1	Status word 2

Status word :

Sw1	**Sw2**	**Meaning**
'90'	'00'	执行成功
'68'	'CX'	PIN 失败，X 表示剩余次数
'69'	'CX'	PIN 验证失败，X 表示剩余次数
'69'	'84'	数据不合法
'6A'	'86'	P1P2 不正确
'6A'	'82'	卡片证书不存在
'6A'	'85'	预制证书不存在
'6A'	'25'	没有 SM4Key
'6A'	'31'	IMEI 值不一致
'6A'	'32'	IMEI 值不存在

Sw1	Sw2	Meaning
'6B'	'01'	没有生成 CSR
'6B'	'13'	没有保存证书
'69'	'99'	SIM 注销
'63'	'10'	获取证书没有结束，请继续取证书
'68'	'82'	验证签名失败
'6B'	'23'	保存证书长度超过指定长度
'6B'	'24'	随机数不存在

A.2 指令

A.2.1 getSimKeyStatus获取SIM状态

卡片接收到该命令后，返回 SIM 卡 ICCID、SIMKEY 版本号和证书状态；

该命令不需要验证 PIN，无上下文逻辑；

Command Message:

Code	Value	Meaning
CLA	'XX'	
INS	'01'	获取 SIMKEY 状态
P1	'00'	
P2	'00'	
Lc	无	
Data	无	
Le	'0D'	返回的字节数

Response Message:

Data Field

Name	Length	Value Description
ICCID	10	例如：98681001161180902652
SIMKEY 版本号	2	例如：1.0 表示为 0100
证书标识	1	0 表示无证书，1 表示有证书

A.2.2 UICC signatur卡签名

卡片接收到该命令时，检查传入的数据长度是否为 42 个字节，前 10 个字节为 ICCID，后 32 个字节为服务器随机数；校验收到的 ICCID 和 SIM 卡 ICCID 是否一致，如果一致使用卡片预制私钥对 ICCID 和随机数进行签名，返回 ICCID 和签名值，如果不一致返回 0x6984 状态字。

该命令不需要验证 PIN，不需要上下文逻辑。

Command Message:

Code	**Value**	**Meaning**
CLA	'XX'	
INS	'02'	随机数签名
P1	'01'	
P2	'00'	
Lc	'2A'	
Data	'xxxx…'	ICCID(10 字节)+随机数（32 字节）
Le	'4A'	返回的字节数

Response Message:

Name	**Length**	**Value Description**
ICCID	10	例如：9868100116118090265 2
签名值	64	

A.2.3 getRandom生成随机数

卡片接收到该命令后，返回 4 字节长度随机数；

Command Message:

Code	**Value**	**Meaning**
CLA	'XX'	
INS	'0B'	生成随机数
P1	'00'	
P2	'00'	
Lc	无	
Data	无	
Le	'04'	返回的字节数

Response Message:

Name	Length	Value Description
随机数	4	例如：21340989

A.2.4 getCSR生成CSR

卡片收到该命令后，首先验证 PIN 是否通过，验证通过之后，获取卡片的 ICCID、生成公私钥对，并生成 CSR 并返回；

该命令需要验证 PIN；

Command Message:

Code	Value	Meaning
CLA	'XX'	
INS	'03'	生成 CSR
P1	'00'	
P2	'00'	
Lc	无	
Data	无	
Le	'FF'	返回的字节数

Response Message:

Name	Length	Value Description
ICCID	10	
随机数	4	
CSR	Var	参考下文表格

CSR 结构说明:

Field	Value Description	
tbsCertificate	Data to be signed	
	Field	Value Description
	version	

	subject	Distinguished Name. DN: cn = iccid 值 s = 省份代码 c = CN
	subjectPublicKeyInfo	Contains the algorithm identifier, parameters and public key value.
signatureAlgorithm	SM3_SM2	
signatureValue	Signature computed accordingly to one of the possible algorithm listed in section **错误!未找到引用源。**	

A.2.5 saveCertificate保存证书

卡片收到该命令后，卡片先检查卡片是否为已经生成过 CSR 文件，并未保存过证书，则把证书保存到 applet 中，否则卡片报错。

该命令需要验证 PIN。

Command Message:

Code	**Value**	**Meaning**
CLA	'XX'	
INS	'04'	保存证书
P1	'11/91'	11 表示后续还有数据，91 表示最后一条数据
P2	'00'	
Lc	Var	
Data	'xxxxx…'	
Le	无	

Response Message:

无

A.2.6 bindSIMKEY绑定关系

该指令用于在保存 ICCID 与终端 IMEI 和终端管理系统以及证书 ID 的关系，这些数据使用服务器随机生成的临时秘钥 Rkey 加密并使用 SM4 算法加密，Rkey 使用卡片公钥加密；

“保存证书命令”执行成功后才可以执行该命令，否则报错；

该命令成功执行后，保存的证书生效，否则保存的证书无效（在个人化过程中，个人化过程未完成；在证书更新过程中，老证书有效）；

该命令需要验证 PIN。

First Command Message:

Code	**Value**	**Meaning**
CLA	'XX'	
INS	'05'	启用证书
P1	'00'	发送签名值
P2	'00'	
Lc	Var	
Data	'xxxx..'	签名值
Le	无	

Response Message:

无

Second Command Message:

Code	**Value**	**Meaning**
CLA	'XX'	
INS	'05'	绑定关系 1
P1	'01'	发送签名原文 1
P2	'00'	
Lc	Var	
Data	'xxxx..'	SM4 秘钥密文
Le	无	

Third Command Message:

Code	**Value**	**Meaning**
CLA	'XX'	GPCS section 11.11
INS	'05'	绑定关系 2
P1	'02'	发送签名原文 2
P2	'00'	
Lc	Var	
Data	'xxxx..'	绑定关系数据密文

Code	Value	Meaning
Le	无	

签名原文由签名原文 1(SM4 秘钥密文)+签名原文 2(绑定关系数据密文)组成，其中绑定关系数据结构如下表所示。

Name	Length	Value Description
ICCID	10	例如：8947010000123456784
IMEI	45	IMEI 转 ACSII 码 (3 个 IMEI 值, 每一个 IMEI 15 字节)
MDMID	3	例如：1.0.0 表示为 010000
证书公钥	64	
证书 ID	Var	1122334455667788

Response Message:

无

A.2.7 PIN操作

A.2.7.1 验证PIN

卡片接收到该命令后，验证 PIN 值，成功返回 9000；如果失败，返回 96xx，xx 表示剩余验证 PIN 次数；如果剩余次数为 0 时，即使 PIN 值正确也无法再验证 PIN；

Command Message:

Code	Value	Meaning
CLA	'XX'	
INS	'06'	PIN 操作
P1	'01'	验证 PIN
P2	'00'	
Lc	Var	
Data	'xxxx…'	PIN 值（6 个字节）
Le	无	

Response Message:

无

A.2.7.2 修改PIN

卡片接收到该命令后，首先验证旧 PIN 是否验证通过，旧 PIN 值不正确或者剩余验证 PIN 次数为 0 都无法修改 PIN；

Command Message：

Code	**Value**	**Meaning**
CLA	'XX'	
INS	'06'	PIN 操作
P1	'02'	修改 PIN
P2	'00'	
Lc	'0C'	
Data	'xxxx…'	旧 PIN（6 字节）+新 PIN（6 个字节）
Le	无	

Response Message:
无

A.2.7.3 重置PIN

First Command Message：

Code	**Value**	**Meaning**
CLA	'XX'	
INS	'06'	PIN 操作
P1	'03'	重置 PIN
P2	'00'	发送签名值
Lc	Var	
Data	'xxxx..'	签名值
Le	无	

Response Message:
无

Second Command Message：

Code	**Value**	**Meaning**
CLA	'XX'	

Code	Value	Meaning
INS	'06'	PIN 操作
P1	'03'	重置 PIN
P2	'01'	发送签名体
Lc	Var	
Data	'xxxx..'	签名原文（除随机数外的签名原文）
Le	无	

签名原文是由加密秘钥密文+重置 PIN 数据密文组成，其中重置 PIN 数据结构如下表所示。

Name	Length	Value Description
ICCID	10	例如：8947010000123456784
Text	6	313233343536

Response Message:

无

A.2.8 读取工业互联网ID

通过工业 ID 索引选定要读取的工业 ID 记录；

生成会话密钥（SM4 加密方式 GMCipher.ALG_SM4_CBC_NOPAD）；

使用会话密钥对工业 ID 数据进行加密，用卡片共钥对会话密钥进行加密密，使用卡片私钥对数据进行数字签名。

Command Message:

Code	Value	Meaning
CLA	'XX'	
INS	'0C'	读取 ID
P1	'0X'	工业 ID 索引值（01-05）
P2	'00'	
Lc	F0	
Data	无	
Le	无'	

Response Message:

Name	Length	Value Description
会话密钥密文	112	“AFE8……7B”
工业 ID 密文	64	“AFE8……7B”（暂定最大长度）
签名值	64	“AFE8……7B”

A.2.9 写入工业互联网ID

通过工业 ID 索引选定要写入的工业 ID 记录;
使用服务器公钥验证签名;
用卡片私钥对会话密钥进行解密（SM4 加密方式 GMCipher.ALG_SM4_CBC_NOPAD）;
使用会话密钥对工业 ID 数据进行解密。

Command Message:

Code	Value	Meaning
CLA	'XX'	
INS	'0D'	写入 ID
P1	'0X'	工业 ID 索引值（01-05）
P2	'00'	
Lc	F0	
Data	“XXXX”	数据体（会话密钥密文+工业 ID 密文+签名）
Le	无'	

Response Message::

Name	Length	Value Description
会话密钥密文	112	“AFE8……7B”
工业 ID 密文	64	“AFE8……7B”（暂定最大长度）
签名值	64	“AFE8……7B”

附　录 B

（规范性附录）

B 型（低性能）通用集成电路卡片指令集

B.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UICC卡。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：

Command Message：

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

Response Message：

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

Status word ：

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

B.2　接口指令集

Command Message：

序号	指令名称	说明
1	GET RAND	获取随机数
2	IMPORT KEY	导入密钥

3	READ IDENTIFIER	读取标识
4	WRITE IDENTIFIER	写入标识
5	DELETE IDENTIFIER	删除标识

B.2.1 获取随机数

定义与范围：该指令用于获取硬件随机数。

Command Message：

字段	值(Hex)	说明
CLA	XX	
INS	0B	获取随机数
P1	00	
P2	00	
Lc	无	
Data	无	
Le	08	

Response Message：

字段	长度	说明
Data	08	随机数数据

Status word ：

SW1	SW2	含义
90	00	执行成功
69	82	安全状态不满足
6A	86	P1或P2参数错
67	00	Lc长度错误

B.2.2 导入密钥

定义与范围：该指令用于工厂生产阶段导入芯片预制密钥。预制密钥包括加解密密钥和签名验签密钥。加解密密钥用于数据传输保护，签名验签密钥用于平台和终端身份认证。

Command Message code：

字段	值(Hex)	说明
CLA	XX	
INS	04	导入密钥
P1	00	
P2	00	
Lc	var	
Data	‘XXXX’	

Le	无	

Command Message：

字段	长度	说明
KeyUsage	1	密钥用途，00加解密，01签名验签
KeyType	1	密钥类型， 00 SM4, 01 AES, 02 TDES,
KeyLen	2	密钥长度
KeyValue	var	密钥值

Response Message：

无

Status word ：

SW1	SW2	含义
90	00	执行成功
6A	80	数据域参数错误
6A	84	空间不足
6A	86	P1或P2参数错
67	00	Lc长度错误

B.2.3 写入标识

定义与范围：该指令属于管理指令，用于生产或售后等管理环节中进行工业互联网标识写入或更新。该指令输入随机数(可选)、主动标识密文、防重放因子、及上述数据签名。

执行该指令时，先验证指令数据的签名合法性，然后对防重放因子进行合法性判断，通过后进行解密标识并写入。

如采用对称密钥算法，使用输入的随机数对解密密钥和签名密钥分散得到会话密钥。用签名会话密钥对所有数据计算签名验证，然后用解密会话密钥解密主动标识密文。

Command Message code：

字段	值(Hex)	说明
CLA	XX	
INS	7D	写入标识
P1	00 01 02	00 算法使用SM4 01 算法使用AES 02 算法使用TDES
P2	00	
Lc	var	
Data	‘XXXX’	
Le	00	

Command Message：

字段	长度	说明
Random	8	随机数，明文
IndustryID	Var	主动标识，密文
Counter	5	防重放因子，密文
MAC	8	以上数据的签名

Response Message：

无

Status word ：

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

B.2.4 读取标识

定义与范围：该指令用于读取工业互联网主动标识。该指令输出随机数（可选）、芯片唯一编码，主动标识，防重放因子、及上述数据签名。

如采用对称密钥算法，指令执行时先获取随机数，用所得随机数分别对加密密钥和签名密钥分散得到会话密钥。外部请求数据用加密会话密钥加密，然后用签名会话密钥对所有数据计算签名值。

Command Message code：

字段	值(Hex)	说明
CLA	XX	
INS	7E	读取标识
P1	00 01 02	00 算法使用SM4 01 算法使用AES 02 算法使用TDES
P2	00	
Lc	00	
Data	无	
Le	var	

Command Message：

无

Response Message：

字段	长度	说明
Random	8	随机数，明文
ICCID	var	卡片唯一编码，明文
IndustryID	var	主动标识，密文
Counter	5	防重放因子，密文
MAC	8	以上数据的签名数据

Status word ：

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

B.2.5 删除标识

定义与范围：该指令属于管理指令，用于售后等管理环节中进行工业互联网标识删除。该指令输入随机数(可选)、主动标识密文、防重放因子、及上述数据签名。

执行该指令时，先对防重放因子进行合法性判断，然后验证指令数据的签名合法性，验证后进行标识删除。

如采用对称密钥算法，使用输入的随机数对签名密钥分散得到会话密钥。用签名会话密钥对所有数据计算签名验证。

Command Message code：

字段	值(Hex)	说明
CLA	XX	
INS	7F	删除标识
P1	00 01 02	00 算法使用SM4 01 算法使用AES 02 算法使用TDES
P2	00	
Lc	var	
Data	‘XXXX’	
Le	00	

Command Message：

字段	长度	说明
Random	8	随机数，明文
IndustryID	var	主动标识，密文
Counter	5	防重放因子，密文
MAC	8	以上数据的签名

Response Message：

无

Status word ：

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