

T/CAICI

中国通信企业协会团体标准

T/CAICI XXXX—XXXX

## 物联网 AI-eSIM 技术要求

Technical requirements for IoT AI-eSIM

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

中国通信企业协会 发布

目 次

前言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 缩略语.....2

5 整体系统架构缩略语.....3

6 卡要求.....4

7 平台要求.....5

8 业务流程.....6

9 接口要求.....8

10 安全要求.....9

参考文献..... 11

索引..... 12

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国通信企业协会标准化管理委员会提出并归口。

本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件起草单位：芯昇科技有限公司、联通华盛通信有限公司、天翼物联科技有限公司、中国电信股份有限公司全渠道运营中心、中国移动通信有限公司研究院、中移物联网有限公司、华为技术有限公司、紫光同芯微电子有限公司、北京中电华大电子设计有限责任公司、上海复旦微电子集团股份有限公司、北京握奇数据股份有限公司、东信和平科技股份有限公司。

本文件主要起草人：肖青、刘梅娟、卢丽敏、陈浩、崇静、刘辉、蒋文隆、王宏、赵军、常志刚、金鑫、叶文莉、曹辉、徐小俊。

本文件为中国通信企业协会首次发布。

# 物联网 AI-eSIM 技术要求

## 1 范围

本文件规定了物联网AI-eSIM系统的业务概述、卡要求、平台要求、接口要求和安全要求。  
本文件适用于物联网场景下支持智能体应用的AI-eSIM卡、终端设备及智能体应用平台的设计、开发、生产、测试和运营。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15852.1—2020 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制  
GB/T 32907—2016 信息安全技术 SM4分组密码算法  
GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求  
ISO/IEC 7816（所有部分） 识别卡 集成电路卡  
ISO/IEC 15408（所有部分） 信息技术 安全技术 信息技术安全评估准则  
3GPP TS 23.048 Security mechanisms for the (U)SIM application toolkit; Stage 2  
3GPP TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application  
3GPP TS 31.111 Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)  
3GPP TS 31.130 (U)SIM API; (U)SIM API for Java Card  
ETSI TS 102.221 Smart cards; UICC-Terminal interface; Physical and logical characteristics  
ETSI TS 102.223 Smart cards; Card Application Toolkit (CAT)  
ETSI TS 102.226 Smart cards; Remote APDU structure for UICC based applications  
ETSI TS 102.241 Smart cards; UICC Application Programming Interface (UICC API) for Java Card  
ETSI TS 102.267 Smart cards; Connection oriented API for Java Card  
IETF RFC 6455 The WebSocket Protocol  
IETF RFC 9110 HTTP Semantics  
GlobalPlatform Card Specification v2.2  
GlobalPlatform Card Specification v2.2 – Amendment B  
GlobalPlatform Card Specification v2.3  
GSMA SGP.32 eSIM IoT Remote Provisioning and Management Specification  
GSMA SGP.22 RSP Technical Specification – Consumer

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

AI-eSIM 卡 AI-eSIM card 支持远程 SIM 配置功能，并具备智能体应用所需安全令牌运算能力的嵌入式用户身份模块。

### 3.2

智能体 agent 能够感知环境并自主采取行动以实现特定目标的实体。

### 3.3

智能体应用平台 agent application platform 面向物联网 AI-eSIM 终端提供智能体应用服务的统一平台。

3.4

AIKEY 存储于 AI-eSIM 卡中，写入后不可直接读取的业务密钥，一卡一密。

3.5

会话密钥 session key 用于单次业务安全令牌计算的临时密钥。

3.6

AI Token 表征大模型能力调用量的计量单位，用于 AI 服务的计量与计费。

3.7

安全令牌 security token 用于身份认证与鉴权的报文鉴别码。

3.8

空中写卡 over-the-air provisioning 通过空中接口向 AI-eSIM 卡远程写入卡个人化数据的过程。

3.9

写卡数据 provisioning data 空中写卡过程中下发至 AI-eSIM 卡的卡个人化数据。

3.10

终端设备 terminal device 内置 AI-eSIM 卡的物联网终端。

3.11

信控 service control 依据用量超套、安全风险等情形实施的服务停服与复通控制。

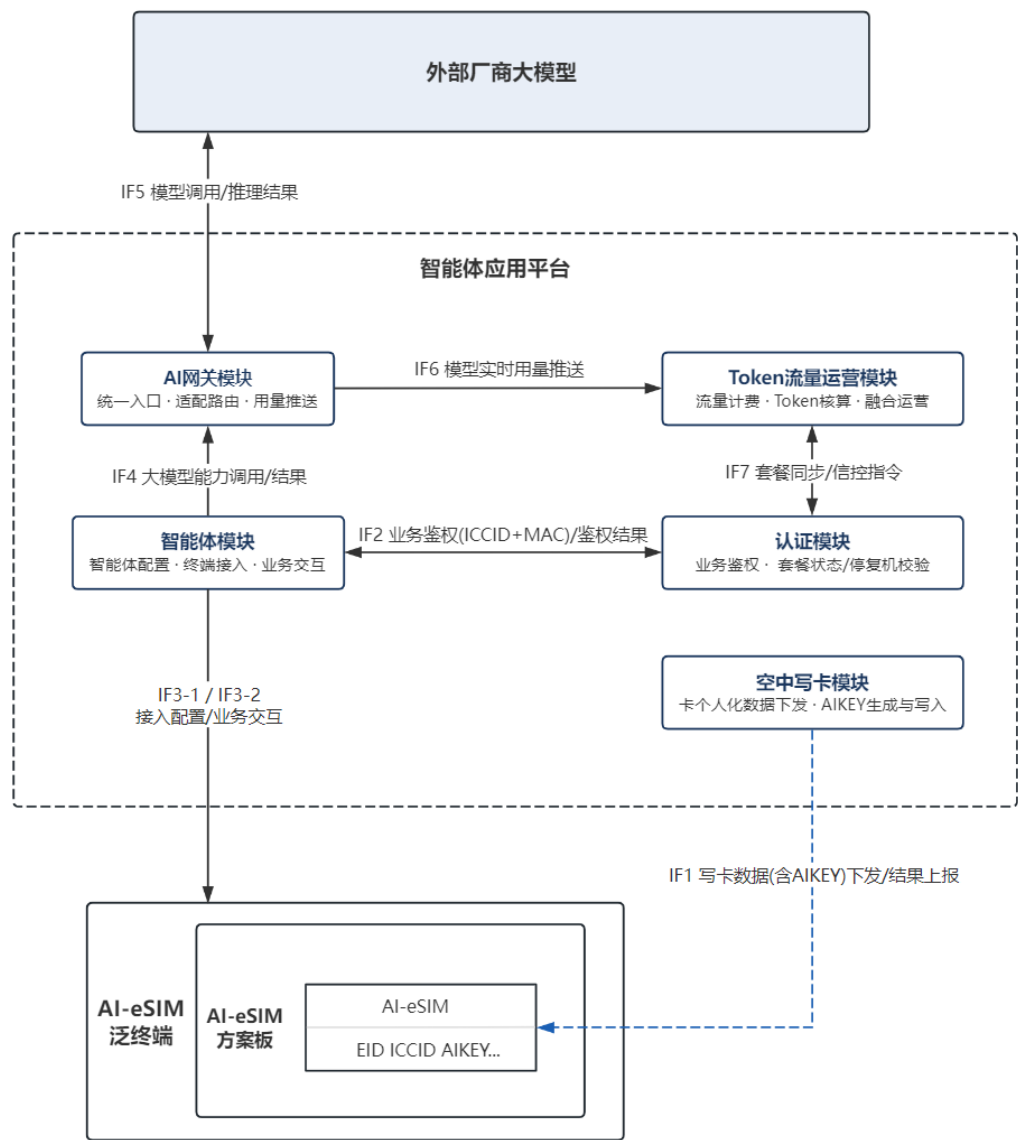
4 缩略语

下列缩略语适用于本文件。

| 缩略语       | 全称与中文说明                                               |
|-----------|-------------------------------------------------------|
| AES       | 高级加密标准 advanced encryption standard                   |
| AI        | 人工智能 artificial intelligence                          |
| API       | 应用程序编程接口 application programming interface            |
| BIP       | 承载无关协议 bearer independent protocol                    |
| COS       | 片内操作系统 chip operating system                          |
| EAL       | 评估保证级 evaluation assurance level                      |
| eUICC     | 嵌入式通用集成电路卡 embedded universal integrated circuit card |
| GP        | 全球平台组织 GlobalPlatform                                 |
| HTTPS     | 超文本传输安全协议 hypertext transfer protocol secure          |
| ICCID     | 集成电路卡标识 integrated circuit card identifier            |
| IMSI      | 国际移动用户标识 international mobile subscriber identity     |
| MAC       | 报文鉴别码 message authentication code                     |
| OTA       | 空中下载 over-the-air                                     |
| PoR       | 收据证明 proof of receipt                                 |
| RAM       | 远程应用管理 remote application management                  |
| RFM       | 远程文件管理 remote file management                         |
| SM4       | 国家密码管理部门认可的分组密码算法（SM4分组密码算法）                          |
| TAR       | 工具包应用参考 toolkit application reference                 |
| UDH       | 用户数据头 user data header                                |
| USAT      | 通用用户身份模块应用工具包 USIM application toolkit                |
| USIM      | 通用用户身份模块 universal subscriber identity module         |
| WebSocket | 基于TCP的全双工通信协议                                         |

5 整体系统架构缩略语

5.1 整体系统架构图



<sup>a</sup> 图1 系统总体架构图

5.1.1 系统构成

物联网AI-eSIM系统由AI-eSIM卡、终端设备、智能体应用平台和大模型能力提供方构成。

5.1.2 功能模块组成

智能体应用平台应由下列功能模块组成：

- a) 空中写卡模块：通过空中方式向AI-eSIM卡写入卡个人化数据；
- b) 认证模块：对智能体业务实施业务鉴权，保证合法终端设备调用AI能力；
- c) 智能体模块：面向AI智能交互终端设备，提供智能体配置管理、终端接入与设备管理，并向终端提供智能交互服务；
- d) Token流量运营模块：统一管理基础通信流量与AI Token服务，实现流量计费、AI Token核算、账单结算、服务订购与管控；
- e) AI网关模块：作为平台对接大模型的统一入口，负责大模型能力的统一对接、适配与路由。

### 5.1.3 建设运营与接口交互

各功能模块可由不同主体建设和运营，并应通过第9章规定的接口交互。

### 5.1.4 参考点与接口对应关系

技术参考模型中的参考点应与表1所列接口一一对应。

## 6 卡要求

### 6.1 总体要求

#### 6.1.1 规格划分

AI-eSIM卡分为A、B两种规格。

#### 6.1.2 A类卡

A类卡应包括（但不限于）下列功能：

- a) 支持ISO/IEC 7816接口；
- b) 支持UICC/USIM功能；
- c) 支持USAT/STK能力；
- d) 支持空中写卡功能；
- e) 支持AI-eSIM应用功能，该功能为COS预制功能。

#### 6.1.3 B类卡

B类卡应包括（但不限于）下列功能：

- a) 支持ISO/IEC 7816接口；
- b) 支持UICC/USIM功能；
- c) 支持USAT/STK能力；
- d) 支持GP；
- e) 支持多应用功能；
- f) 支持空中写卡功能；
- g) 支持AI-eSIM应用功能，该功能由卡应用承载。

### 6.2 硬件要求

#### 6.2.1 物理、电气和逻辑特性

AI-eSIM卡的物理、电气和逻辑特性应符合ETSI TS 102.221的规定。

#### 6.2.2 接口特性

AI-eSIM卡的接口应符合ISO/IEC 7816的规定。

### 6.3 COS要求

#### 6.3.1 远程SIM配置功能要求

应支持远程SIM配置功能，并应符合GSMA SGP.22或 SGP.32的规定。

#### 6.3.2 连接功能要求

##### 6.3.2.1 UICC要求

应支持UICC功能，并应符合ETSI TS 102.221的规定。

##### 6.3.2.2 USIM要求

应支持USIM功能，并应符合3GPP TS 31.102的规定。

##### 6.3.2.3 USAT要求

应支持USAT功能，并应符合ETSI TS 102.223和3GPP TS 31.111的规定。

##### 6.3.2.4 BIP及相关协议要求

应支持BIP功能，并应符合ETSI TS 102.223、ETSI TS 102.226、ETSI TS 102.267和GlobalPlatform Card Specification v2.2 – Amendment B的规定。

##### 6.3.2.5 RAM/RFM要求

应支持通过短信或BIP方式实现RAM/RFM功能，并应符合ETSI TS 102.226的规定。

#### 6.3.3 多应用要求

##### 6.3.3.1 跨平台多应用运行时环境要求

支持多应用功能的AI-eSIM卡应支持跨平台多应用运行时环境，保证卡应用与芯片及COS独立，使同一个应用可以在不同厂商的eUICC卡下载及运行。

#### 6.3.3.2 GP要求

应支持GP功能，并应符合GlobalPlatform Card Specification v2.2的规定。

#### 6.3.3.3 API要求

##### 6.3.3.3.1 基础API要求

应支持跨平台多应用运行时环境基础编程API，包括应用框架、通信接口、加解密算法等基础功能。

##### 6.3.3.3.2 UICC API要求

应支持UICC API，并应符合ETSI TS 102.241的规定。

##### 6.3.3.3.3 USIM API要求

应支持USIM API，并应符合3GPP TS 31.130的规定。

##### 6.3.3.3.4 GP API要求

应支持GP API、GP Card Contactless API，并应符合GlobalPlatform Card Specification v2.3的规定。

##### 6.3.3.3.5 连接服务API要求

应支持连接服务API，支持SCP81 Connection，并应符合ETSI TS 102.267的规定。

#### 6.4 应用要求

##### 6.4.1 安全令牌功能要求

应支持生成安全令牌功能，生成方法与报文格式应符合9.3的规定。

##### 6.4.2 OTA要求

应支持BIP协议，包括支持Setup Event List(Data Available、Channel Status、Location Status)、ENVELOPE (EVENT DOWNLOAD—Data Available、Channel Status、Location Status)，主动式命令Open Channel、Send Data、Receive Data、Close Channel、Refresh，并应符合ETSI TS 102.223的规定。

##### 6.4.3 安全报文要求

应支持安全报文，并应符合3GPP TS 23.048的规定。命令数据应符合表2的规定。

##### 6.4.4 获取会话密钥指令

###### 6.4.4.1 指令用途

终端应通过获取会话密钥指令获取会话密钥。终端和智能体应用平台进行业务交互的过程中，该密钥分散后用于对业务数据计算MAC。

###### 6.4.4.2 执行条件

获取会话密钥指令的执行条件如下：

- a) 在01通道上选择应用后执行；
- b) 使用指令给出的分散因子，补充Pad后通过SM4-CBC算法产生会话密钥。

###### 6.4.4.3 报文格式

命令请求格式应符合表3的规定，响应信息及状态码应符合表4的规定。

###### 6.4.4.4 密钥生成

应采用SM4-KDEC密钥使用SM4-CBC算法对分散因子数据及其补位进行加密，获取一个会话密钥作为响应。

#### 6.5 Profile要求

应支持AI-eSIM密钥个人化，密钥个人化宜通过ProcessData接口写入。

## 7 平台要求

### 7.1 总体要求

智能体应用平台应由空中写卡模块、认证模块、智能体模块、Token流量运营模块和AI网关模块组成，各模块的组成与定位应符合5.1.2的规定。

智能体应用平台应具备空中写卡、业务鉴权、智能体服务、用量运营和大模型能力汇聚等功能，各功能模块的要求应符合7.2~7.6的规定。

各功能模块可由不同主体建设和运营，并应通过第9章规定的接口交互。

### 7.2 空中写卡模块

空中写卡模块中码号数据远程配置的流程、报文格式和通道安全，应符合GSMA SGP.22或SGP.32及现行相关行业标准的规定，本文件仅规定与智能体应用相关的AIKEY写入要求。

空中写卡模块应支持在写卡数据中包含AIKEY字段，并应支持AIKEY与卡个人化数据按卡标识(ICCID)关联、导入和下发。

AIKEY应在受控的安全环境中生成，并应以密文形式存储和传输。

### 7.3 认证模块

认证模块应支持MAC校验运算，MAC的计算和校验应符合9.4的规定。

认证模块应对智能体业务实施业务鉴权，校验不通过的应拒绝。

认证模块应支持接收Token流量运营模块同步的AI套餐订购信息和下发的信控指令，并应维护终端设备的套餐订购状态和停复机状态。

### 7.4 智能体模块

智能体模块应提供接入配置接口和业务交互接口，应符合IETF RFC 9110和IETF RFC 6455的规定。

终端接入时，智能体模块应调用认证模块完成业务鉴权，鉴权通过后方可建立业务交互，鉴权不通过的应拒绝。

智能体模块应支持接收终端上传的业务报文并下发处理结果，业务数据传输应采用加密通道，应通过AI网关模块调用大模型能力。

智能体模块应支持智能体的生命周期管理。

### 7.5 Token流量运营模块

#### 7.5.1 流量运营

应支持基础通信流量的实时计量和多模流量的实时监测，并应支持流量消耗异常的检测和告警。

应支持流量单独计费，并应支持预付费和后付费计费模式。

#### 7.5.2 AI Token运营

应支持接收AI网关模块推送的模型实时用量，并应支持对用量异常的检测和告警。

应支持按AI Token用量单独计费，并应支持预付费和后付费计费模式。

#### 7.5.3 融合运营

应支持融合套餐的定义、上架、订购、退订和暂停，实现套餐的全生命周期管理。

应支持流量与AI Token融合计费。

应根据用量超套、存在安全风险等情形实施信控。

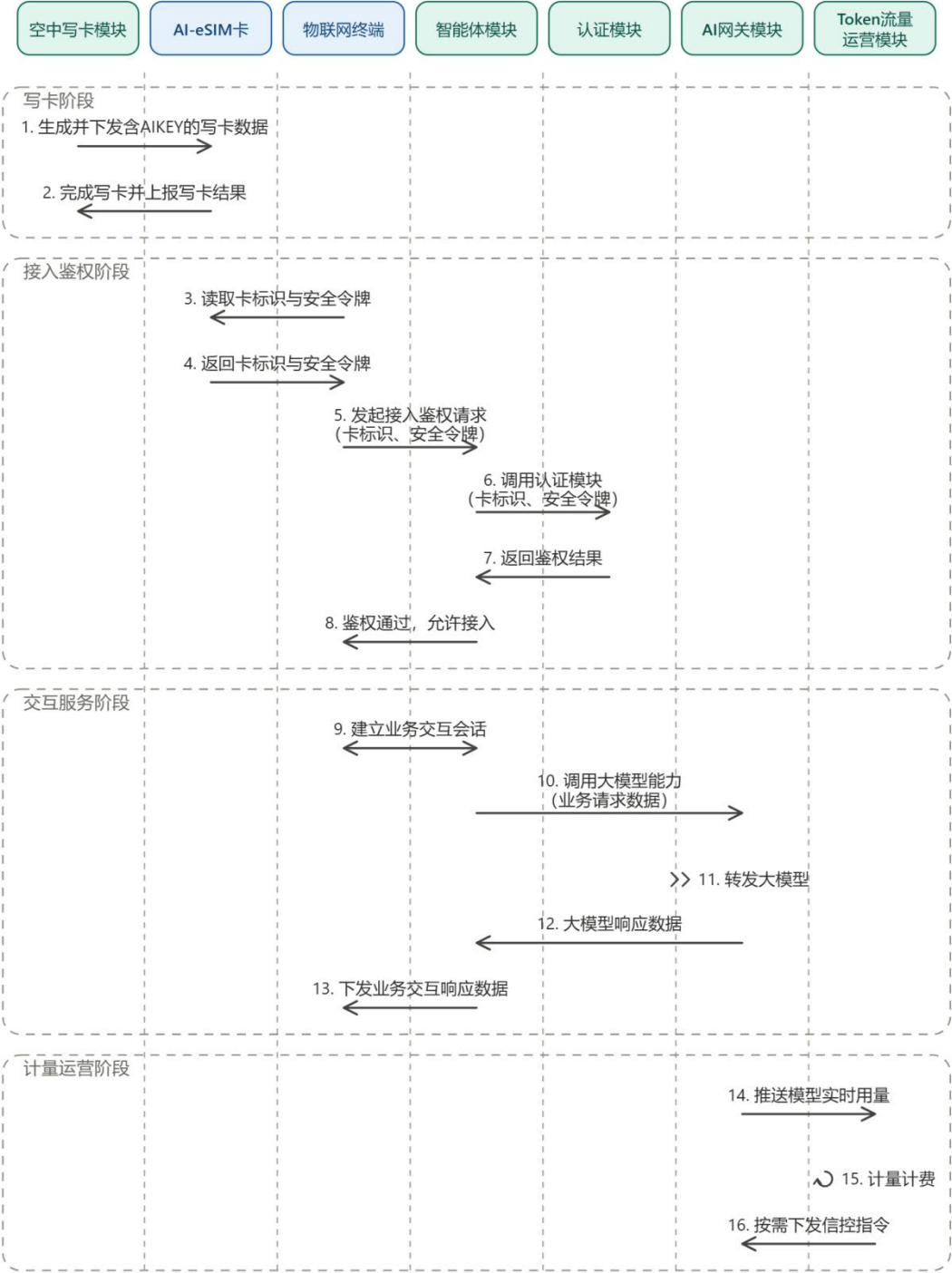
### 7.6 AI网关模块

应支持对接不同模型厂商的异构大模型能力，并应支持将调用请求路由至对应的大模型。

AI网关模块应支持大模型能力实时计量用量推送至Token流量运营模块。

## 8 业务流程

8.1 整体业务流程如下图2所示：



<sup>b</sup> 图 2 业务流程图

a) 写卡阶段: 空中写卡模块生成并下发含AIKEY的写卡数据, AI-eSIM卡完成写卡并上报写卡结果;

b) 接入鉴权阶段: 终端经智能体模块携带卡标识和安全令牌调用认证模块完成业务鉴权;

- c) 交互服务阶段：鉴权通过后，终端与智能体模块建立业务交互，由智能体模块经AI网关模块调用大模型能力；
- d) 计量运营阶段：AI网关模块推送模型实时用量，Token流量运营模块完成计量计费并按需下发信控指令。

8.2 流程与接口对应关系

各阶段涉及的接口调用应符合9.2的规定，交互失败时应按9.1的异常处理与重试机制处理。

9 接口要求

9.1 接口通用要求

9.1.1 异常处理与重试

接口应具备异常处理与重试机制。

9.1.2 版本兼容

接口应采用版本化设计并向下兼容，应支持与不同版本系统及不同厂商设备的对接。

9.1.3 交互日志

接口应建立日志记录机制，记录内容应符合以下要求：

- a) 访问日志应记录请求时间、来源标识、目标标识、请求类型及交互结果；
  - b) 操作日志应记录操作主体、操作对象、操作内容、操作时间及操作结果；
  - c) 业务日志应记录业务类型、关键参数摘要、处理结果及异常信息。
- 日志的留存期限、敏感信息保护、完整性保护及访问控制等安全要求应符合10.5的规定。

9.1.4 通信安全

接口通信安全应符合第10章的规定。

9.2 平台核心接口

9.2.1 接口定义

平台核心接口的定义见表1。接口的具体协议和数据格式由对接双方约定，本文件规定各接口的交互用途。

9.2.2 接口符合性

IF3-1和IF3-2应分别符合7.4.1中对接入配置接口和业务交互接口的规定。

表1 平台核心接口定义

| 接口    | 交互双方                  | 归属模块        | 核心用途                            |
|-------|-----------------------|-------------|---------------------------------|
| IF1   | AI-eSIM卡与空中写卡模块       | 空中写卡模块      | 写卡数据（含AIKEY）下发与写卡结果上报           |
| IF2   | 智能体模块与认证模块            | 认证模块        | 业务鉴权请求（含ICCID和MAC值）与鉴权结果返回      |
| IF3-1 | 终端设备（含AI-eSIM卡）与智能体模块 | 智能体模块       | 接入配置接口（HTTPS）：连接信息、访问凭证与服务器时间获取 |
| IF3-2 | 终端设备（含AI-eSIM卡）与智能体模块 | 智能体模块       | 业务交互接口业务数据上传与结果数据下发、控制消息交互      |
| IF4   | 智能体模块与AI网关模块          | AI网关模块      | 大模型能力调用请求与结果返回                  |
| IF5   | AI网关模块与模型厂商的大模型       | AI网关模块      | 模型调用请求转发与推理结果返回                 |
| IF6   | AI网关模块与Token流量运营模块    | Token流量运营模块 | 模型实时用量推送                        |
| IF7   | Token流量运营模块与认证模块      | 认证模块        | AI套餐订购信息同步与信控指令（停服、复通）下发        |

9.3 卡端安全报文接口

9.3.1 报文结构

命令报文结构应符合3GPP TS 23.048的规定。

9.3.2 命令数据

命令数据应符合表2的规定。

表2 命令数据

| 数据域  | 类型  | M/O | 长度<br>(字节) | 示例                                                               |
|------|-----|-----|------------|------------------------------------------------------------------|
| 命令类型 | HEX | M   | 1          | 0xB1: 卡端身份认证与鉴权; 0xB2: 平台身份认证与鉴权; 0xB3: 平台响应认证结果; 0xB4: 卡端响应认证结果 |
| 命令长度 | HEX | M   | 1          | 后续命令参数的长度                                                        |
| 命令参数 | HEX | M   | XX         | 具体内容参见9.3.3                                                      |

注: M: 必备; O: 可选。

9.3.3 获取会话密钥指令

9.3.3.1 命令请求

获取会话密钥命令请求格式应符合表3的规定。

表3 获取会话密钥命令请求

| 字段   | 值           | 说明     |
|------|-------------|--------|
| CLA  | 80          | —      |
| INS  | 51          | —      |
| P1   | 00          | —      |
| P2   | 00          | —      |
| Le   | XX (小于16字节) | 预期响应长度 |
| Data | 分散因子数据      | —      |

9.3.3.2 状态码

获取会话密钥指令的状态码应符合表4的规定。

表4 获取会话密钥指令状态码

| 状态码  | 说明        |
|------|-----------|
| 6E00 | CLA错误     |
| 6D00 | INS错误     |
| 6A86 | P1、P2参数错误 |
| 6700 | Lc错误      |
| 6F00 | 接收数据错误    |

9.4 算法要求

AI-eSIM应支持符合GB/T 32907—2016规定的SM4算法; 可支持AES算法。

MAC值的计算和校验应符合GB/T 15852.1—2020的规定。

10 安全要求

10.1 芯片安全

AI-eSIM卡芯片应通过EAL4+(含)以上安全认证, 并应涵盖各类算法的安全检测, 评估应符合ISO/IEC 15408的规定。

支持多应用功能的AI-eSIM卡芯片应通过EMVCo安全认证, 或通过银联芯片卡集成电路安全测试。

10.2 COS安全

AI-eSIM卡COS应通过EAL4+ (含) 以上安全认证, 评估应符合ISO/IEC 15408的规定。

支持多应用功能的AI-eSIM卡应通过eSIM漏洞安全检测。

#### 10.3 密码应用与密钥管理

密码应用应符合GB/T 39786—2021的规定。

根密钥不应出密码机，不应以明文形式存储和传输。

#### 10.4 通信与接口安全

通信接口应采用加密通道。

接口调用应进行身份识别与授权，未获授权的调用应拒绝。

#### 10.5 日志安全

日志的留存期限应符合国家网络安全相关标准及运营要求，且宜不少于6个月，安全日志宜不少于12个月。

各类日志均不应记录AIKEY、会话密钥、写卡数据明文等敏感密钥材料，不应记录完整的业务明文载荷；对用户身份标识等敏感信息，记录与展示时应进行脱敏处理。

日志存储应采取防篡改措施，安全日志宜采用基于SM4的MAC机制或数字签名保障完整性，密码应用应符合GB/T 39786—2021的规定。

日志文件仅允许授权运维及审计人员访问，未获授权的访问应拒绝。

## 参 考 文 献

## 索 引