ICS 67.140.10
CCS X 55

团　　体　　标　　准

T/OIDAA XXX—XXXX

基于SIM卡的数字身份 SIM卡技术要求

SIM-based digital identity SIM card interface requirements

Version 1.0.0

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中关村安信网络身份认证产业联盟　　发 布

目　次

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》给出的规则起草。

请注意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。

本文件由中关村安信网络身份认证产业联盟提出并归口。

本文件起草单位：中移动金融科技有限公司、北京中盾安信科技发展有限公司、联通在线信息科技有限公司、天翼电子商务有限公司、兴唐通信科技有限公司、恒宝股份、厦门中盾安信科技有限公司、北京中电华大电子设计有限责任公司、科道芯国智能技术股份有限公司、北京握奇数据股份有限公司、紫光同芯微电子有限公司、楚天龙股份有限公司、上海复旦微电子集团股份有限公司。

起草人：果艳红、王性国、王昊、庄怀宇、唐欢、张新彬、高诚、梁斌、张林、梁栋、蔡子凡、许雪姣、吕征、张开拓、于克兵、杜平、李金萍、孙亨博、朱志高、叶文莉。

引 言

基于SIM卡的数字身份是一种经过居民身份网络认证服务系统权威认证，存储在运营商SIM卡的可信身份信息。SIM卡具有自主可控、安全存储、安全计算、安全通信等特性，作为数字身份的安全载体，不仅满足数字身份安全存储的需求，还能与身份鉴别设备进行NFC通信提供便捷的自然人身份鉴别服务，为居民身份网络认证服务系统提供多元化的身份认证应用模式。此外，依托SIM卡能进一步有效保护个人数字资产，推动数据要素的安全、高效流通，加速构建新型数字生活。

为统一规范SIM卡提供身份鉴别凭证存储和读取的能力，指导SIM卡进行硬件、COS的开发、测试和使用，并定义SIM卡的硬件要求、COS要求、应用支撑要求等，特制定本部分。

基于SIM卡的数字身份 SIM卡技术要求

1 范围

本文件规定了基于SIM卡的数字身份中以SIM卡作为信息处理载体，所需具备的通用技术要求。

本文件适用于基于SIM卡的数字身份生态应用，并适用于相关系统的设计、开发、测试和应用。

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 32907—2016 信息安全技术 SM4分组密码算法

GB/T 0009—2023 SM2密码算法使用规范

GB/T 42573—2023 信息安全技术 网络身份服务安全技术要求

T/OIDAA xx-xxxx 基于SIM卡的数字身份 技术框架

T/OIDAA xx-xxxx 基于SIM卡的数字身份 NFC身份鉴别流程

T/OIDAA xx-xxxx 基于SIM卡的数字身份 SIM卡接口要求

T/OIDAA xx-xxxx 基于SIM卡的数字身份 身份鉴别设备专用安全芯片应用接口要求

T/OIDAA xx-xxxx 基于SIM卡的数字身份 身份鉴别服务接口要求

T/OIDAA xx-xxxx 基于SIM卡的数字身份 身份鉴别设备专用安全芯片技术要求

T/OIDAA xx-xxxx 基于SIM卡的数字身份 移动终端技术要求

T/OIDAA xx-xxxx 基于SIM卡的数字身份 身份鉴别设备技术要求

3 术语和定义

T/OIDAA XXX—XXXX《基于SIM卡的数字身份 技术框架》界定的术语和定义适用于本文件。

3.1 缩略语

下列缩略语适用于本文件，其他缩略语请参考《SIM 数字身份 XXXXXXX》。

AID 应用标识符（Application IDentifier）

APDU 应用协议数据单元（Application Protocol Data Unit）

API 应用编程接口（Application Programming Interface）

BIP 独立承载协议(Bearer Independent Protocol)

COS 智能卡操作系统 （Chip Operation System）

CLF 非接协议端到端接口 Contactless Front-end (CLF) Interface;

RFM 远程文件管理(Remote File Management)

RAM 远程应用管理(Remote Application Management)

STK SIM应用工具包 （SIM Application Toolkit）

SIM 用户身份识别模块（Subscriber Identity Module）

SWP 单线协议（Single Wire Protocol）
SEID 安全模块标识(Security Environment Identifier)
TAR 工具包应用参考参数 (Toolkit Application Reference)
USIM 通用用户身份识别模块（Universal Subscriber Identity Module）
UICC （Universal Subscriber Identity Module）
USAT USIM应用工具包(USIM Application Toolkit）

4 技术架构

SIM卡技术架构如图1所示，包括：硬件层、COS层、应用基础能力层和应用层四部分

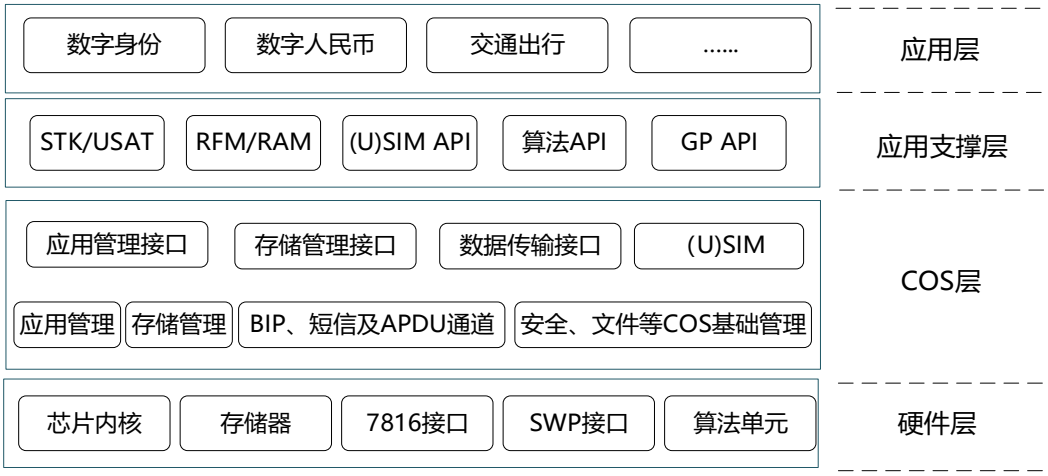

图 1 SIM卡技术架构

4.1 硬件层

定义SIM卡物理层访问接口，包括IO、CPU、存储器、算法单元等。

4.2 COS层

定义SIM卡内存管理、应用管理、各类安全机制、SIM/USIM逻辑功能、空中短信传输协议控制等。

4.3 应用支撑层

定义支持供上层应用调用的各类API等。

4.4 应用层

主要承载各类应用，包含各类行业应用（如公交、金融、校企等），应用可预置也可动态加载。

5 技术要求

5.1 硬件要求

5.1.1 芯片安全要求

SIM卡在芯片选型上应具备以下安全要求：

a) EAL4+以上（含）安全认证；
b) EMVCo 或银联卡芯片安全认证；
c) 国密二级以上（含）安全认证。

5.1.2 物理电气性要求

a) 物理特性、电气特性遵循 ETSI 102.221 的要求；
b) SIM 卡和 CLF 芯片的接口电压，应保证至少支持 Class B 和 C。

5.1.3 通信接口

通信接口指的是 SIM 卡与外部终端设备进行通信的接口，应支持：

a) ISO7816，遵循 ETSI 102.221 的要求；
b) SWP 遵循 ETSI TS 102.613。

5.2 COS 要求

5.2.1 基础功能

a) 采用 UICC 多应用架构要求，支持 SIM 和 USIM 功能，符合 3GPPTS 31.101 和 31.102 要求，同一时刻只能有一个应用处于激活状态；
b) 支持 USAT/STK 指令及功能；
c) 可支持 7816 接口高速通信，如分频参数(F,D) = (512,32)。

5.2.2 物理通道和协议

a) 支持 SWP 和 ISO7816 协议；
b) 多应用在不同协议处理间处理互不影响；
c) 支持混合模式下(SWP 和 7816 协议)的状态切换，保证切换前后的应用状态不受影响；

5.2.3 多逻辑通道

a) 至少支持 4 个逻辑通道（逻辑通道号 0-3）；
b) 支持多逻辑通道同时对不同安全域建立安全通道；

5.2.4 安全算法

支持国家商用密码算法及国际算法；

a) 国家商用密码算法：支持 SM2、SM3、SM4；
b) 国际算法：RSA、ECC、DES、AES；
c) 摘要算法：SHA-1、SHA256、SHA384、SHA512。

5.2.5 多应用管理

OS 应支持应用后下载，且具备防火墙机制，保证应用间安全。

5.3 应用支撑

本章节所有涉及相关能力均符合SIM卡产品相关运营商企业标准。

5.3.1 应用工具包

a) 支持 USAT；
b) 支持 STK。

5.3.2 算法 API

至少支持本规范5.2.4章节涉及的算法，技术要求如下：

a) 支持国密算法 API；
b) 支持国际算法 API；

c） 支持摘要算法 API。

5.3.3 支撑层 API

a） 支持 UICC API；

b） 支持 USIM API；

c） 支持 GP API；

5.3.4 SEID

应具备唯一的 SEID 码：

a） 非授权读取；

b） 授权更新；

5.3.5 TAR

需针对数字身份应用分配唯一的 TAR 值，并唯一关联数字身份 AID。

6 应用层

在满足运营商SIM卡空间管理的基础上，SIM卡支持符合上述规范开发的各类行业应用。

参 考 文 献

[1] ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics
[2] ETSI TS 102.613 Smart Cards; UICC - Contactless Front-end (CLF) Interface;Part 1: Physical and data link layer characteristics