ICS 67.140.10 点击此处添加 ICS 号
CCS X 55

团　　体　　标　　准

T/OIDAA XXX—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

Digital identity based on SIM card

Technical Requirements of the Dedicated Security Chip for Identity

Authentication Equipment

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：北京中电华大电子设计有限责任公司、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、紫光同芯微电子有限公司、兴唐通信科技有限公司、上海复旦微电子集团股份有限公司、厦门中盾安信科技有限公司、北京握奇数据股份有限公司、楚天龙股份有限公司、芯昇科技有限公司。

起草人：李旦、盖树天、于克兵、金鑫、王性国、果艳红、刘金地、廖少翔、梁斌、张林、高云鹏、蔡子凡、许雪姣、刘枫、俞晨煌、赵轶、李伯茹、徐璐。

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。

为统一规范身份鉴别设备专用安全芯片提供鉴权认证和数据交互的能力，指导身份鉴别设备安全芯片的设计和开发，并定义身份鉴别设备安全芯片的封装、引脚等要求，特制定本标准。

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

1 范围

本文件规定了身份鉴别设备专用安全芯片的封装、引脚定义等要求。
本文件适用于身份鉴别设备专用安全芯片的设计、开发、测试和应用。

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 16649.1 识别卡 带触点的集成电路卡 第1部分：物理特性

GB/T 16649.2 识别卡 带触点的集成电路卡 第2部分：触点的尺寸和位置

GB/T 16649.3 识别卡 带触点的集成电路卡 第3部分：电信号和传输协议

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 0009—2023 SM2密码算法使用规范

3 缩略语

T/OIDAA XXXXX 《基于SIM卡的数字身份 技术框架》界定的缩略语适用于本文件。

CLK 时钟（clock）
GND 地（ground）
I/O 输入/输出（input/output）
RST 复位（reset）
VCC 电源电压（supply voltage）

4 术语和定义

GB/T 16649.1、GB/T 16649.2、GB/T 16649.4、GB/T 25069、GB/T 29246、T/OIDAA XXXXX界定的术语和定义适用于本文件。

4.1

安全芯片 Secure Element
含有密码算法、安全功能，可实现密钥管理、算法执行、数据安全存储及通信功能的集成电路芯片。

5 总体架构

图 1 身份鉴别设备专用安全芯片系统架构

身份鉴别设备专用安全芯片系统架构由安全芯片生产厂商、安全芯片管理厂商、设备厂商、应用场景方和移动终端组成，各部分要求如下：

a) 安全芯片生产厂商：负责生产、初始化安全芯片，向安全芯片管理厂商登记芯片信息；
b) 安全芯片管理厂商：负责安全芯片的登记、授权认证、注销等服务以及授权配置、查询、统计等运营管理的能力；
c) 设备厂商：负责生产集成安全芯片的身份鉴别设备；
d) 应用场景方：通过身份鉴别设备提供基于 SIM 卡的数字身份的业务应用；
e) 移动终端：移动终端中的 SIM 卡与身份鉴别设备进行 NFC 通信实现便捷的自然人身份鉴别。

6 安全芯片基本要求

6.1 安全芯片整体要求

安全芯片整体要求如下：

a) 应具备独立安全内核；
b) 应具备专用密码算法硬件计算单元；
c) 应具备防御侵入式/半侵入式攻击、侧信道分析、故障注入攻击能力，保护敏感信息不被物理攻击设备获取和篡改。

6.2 安全芯片算法要求

安全芯片采用国家密码管理机构核准的密码算法，应支持 SM2、 SM3、 SM4 算法。

6.3 接口要求

安全芯片提供通用物理传输接口进行安全数据交互，接口应支持 ISO7816。

6.4 通信协议要求

安全芯片的通信协议应符合《GB/T 16649.3—2006 识别卡 带触点的集成电路卡 第 3 部分： 电信号和传输协议》的要求。

6.5 空间要求

安全芯片应提供的用户可用空间不小于 16KB。

6.6 安全认证要求

安全芯片安全认证要求如下：

a) 安全芯片应通过 EAL4+或以上认证；
b) 安全芯片应通过国家商用密码产品二级认证。

6.7 硬件参数要求

安全芯片硬件参数要求如下：

a) 工作环境温度：-25℃ ~ 85℃（消费级）/-40℃ ~ 105℃（工业级）；
b) 工作电压（VCC）：1.62V ~ 5.5V；
c) 支持 Standby 省电模式，Standby 功耗小于 200uA。

7 封装及引脚定义

7.1 PSAM 卡形态布局

PSAM 卡形态布局要求见图 2。

图 2 PSAM 卡形态布局

7.2 电路封装形态及引脚定义

7.2.1 单 7816 产品

单 7816 电路产品采用 QFN32（4X4X0.75-0.4）封装形态，见图 3。

图 3 单 7816 QFN32 封装形态

单 7816 电路产品引脚定义，见表 1。

表 1 单 7816 QFN32 引脚信息

封装引脚编号	引脚名称	引脚描述
1	GND	接触地引脚
2	7816_IO	接触 IO 引脚，上电默认为输入态、带内部上拉电阻
3	NC	
4	NC	
5	NC	
6	NC	
7	NC	
8	NC	
9	NC	

10	NC	
11	NC	
12	NC	
13	NC	
14	NC	
15	NC	
16	NC	
17	NC	
18	NC	
19	NC	
20	NC	
21	CLK	接触时钟引脚，带内部下拉电阻
22	RST	接触复位引脚，带内部下拉电阻
23	VCC	接触电源引脚
24	NC	
25	NC	
26	NC	
27	NC	
28	NC	
29	NC	
30	NC	
31	NC	
32	NC	

7.3 关键尺寸

QFN32 封装形态电路产品关键尺寸见图 4。

图 4 QFN32（4X4X0.75-0.4）封装关键尺寸

7.4 产品丝印

产品丝印一般都有 PIN1 标识，丝印定义为 XXYYWWW，其中 XX 为供应商代码，YYWW 代表年、周。

参 考 文 献

[1] JR/T 0025—2018　中国金融集成电路（IC）卡规范