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卡接口要求

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、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、楚天龙股份有限公司、北京握奇数据股份有限公司、北京中广瑞波科技股份有限公司、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、倪萌、高诚、刘金地、梁斌、张林、梁栋、蔡子凡、许雪姣、吕征、叶璇、苑中魁、张硕、李伯茹、李中敏、周鹏、李娟娜。

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，并指导用户进行鉴别设备软件开发、对接和使用，并定义身份认鉴别设备与SIM卡之间交互时的数据结构和指令格式等，特制定本部分。

基于SIM卡的数字身份 SIM卡接口要求

1 范围

本文件规定了基于SIM卡的数字身份的SIM卡接口要求，并对相关业务类型、业务标签、指令等进行定义和描述。

本文件适用于基于SIM卡的数字身份中与SIM卡交互部分，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 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 SIM卡技术要求

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、定义和缩略语

3.1 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。

3.2 缩略语

AID 应用标识符（Application Identifier）

MAC 消息校验码（Message Authentication Code）

BIP 承载独立协议（BEARER INDEPENDENT PROTOCOL）

SIM 用户识别卡（Subscriber Identity Module）

NISSA 网络身份安全空间地址（Network Identity Security Space Address）

4 业务类型

表 1 业务类型

业务类型	类型值	说明
身份鉴别凭证	FC	用于身份鉴别凭证数据写入、更新及读取

5 业务标签

表 2 业务标签

类型	标签	长度(字节)	描述
通用	40	27	NISSA
	42	8	随机数
	43	2	密钥版本
	44	3	应用版本
	45	1	应用状态：0 初始，1 个人化，2 冻结
证书与非对称密钥	91	147	SIM 卡证书
	93	169	身份认证安全芯片授权证书
NFC 场景中间参数	83	64	签名值,原始签名数据
	84	变长	随机数密文： 若使用公钥加密，则长度为 104； 若使用对称密钥加密，则长度为 16。
身份鉴别凭证	50	128	身份鉴别凭证数据

6 命令说明

6.1 命令格式

6.1.1 命令组成

表 3 命令组成

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

6.1.2 命令格式分类

表 4 命令格式分类

格式	命令组成
CASE 1	CLA INS P1 P2
CASE 2	CLA INS P1 P2 Le
CASE 3	CLA INS P1 P2 Lc Data
CASE 4	CLA INS P1 P2 Lc Data Le

6.2 响应格式

表 5 响应格式

数据	状态码	
DATA	SW1	SW2

DATA ：响应数据；
SW1、SW2：卡片执行命令的响应状态码。

7 应用指令

7.1 SELECT 指令

7.1.1 功能描述

此指令用于选择SIM数字身份卡应用。

7.1.2 命令格式

表 6 SELECT 指令

数据	描述
CLA	00
INS	A4
P1	04
P2	00
LC	应用实例 AID 长度
DATA	应用实例 AID
LE	00

7.1.3 响应格式

当相关信息内容未初始化时，以默认值信息返回。

表 7 SELECT 指令响应格式

字段	长度（TLV 格式）			描述
应用版本	1	1	3	xyz
NISSA ID	1	1	27	默认值是全 FF
密钥版本号	1	1	2	默认值是全 FF
应用状态	1	1	1	默认值是全 FF（安装完的初始状态）

7.2 NFC INIT 指令

7.2.1 命令格式

表 8 NFC INIT 指令

数据	描述
CLA	80
INS	CD
P1	XX
P2	00
LC	数据域长度
DATA	数据域
LE	00

a) P1 参数描述：

表 9 NFC INIT P1 描述

b8	b7	b6	b5	b4	b3	b2	b1	说明
0	-	-	-	-	-	-	-	获取第一组或全部数据
1	-	-	-	-	-	-	-	获取下一组数据

b) 数据域格式如下表所示：

表 10 数据域格式

数据域	长度（TLV 格式）			值	M/O
随机数 RANDA	1	1	8	明文	M
身份认证安全芯片授权证书	1	2	169		M

7.2.2 响应格式

表 11 响应格式

数据项	长度（TLV 格式）			值	M/O
*RANDB	1	1	104	密文	M
SIM 卡证书	1	2	147	明文	M
签名	1	1	64	SIM 卡私钥对*RANDB~SIM 卡证书的签名（原始签名数据）	M

7.3 NFC AUTH 指令

7.3.1 命令格式

表 12 NFC AUTH 指令

数据	描述
CLA	80
INS	CE
P1	00
P2	00
LC	数据域长度
DATA	数据域
LE	无

a) 数据域格式如下表所示：

表 13 数据域格式

数据项	长度（TLV 格式）			值	M/O
签名	1	1	64	使用身份认证安全芯片的私钥对{RANDA|RANDB}的签名，签名值为原始签名数据	M

7.3.2 响应格式

无

7.3.3 响应状态码

表 14 NFC AUTH 响应状态码

SW	描述
9000	认证成功
9304	签名无效
6283	应用锁定
6A86	P1P2 参数错误

7.4 NFC GET DATA 指令

7.4.1 功能描述

此指令用于NFC方式读取用户身份鉴别凭证信息。

7.4.2 命令格式

表 15 NFC GET DATA 指令

数据	描述
CLA	80
INS	CF
P1	XX
P2	00
LC	数据长度

DATA	数据域
LE	00

a) P1 参数如下表所示：

表 16 NFC GET DATA 指令

b8	b7	b6	b5	b4	b3	b2	b1	说明
0	-	-	-	-	-	-	-	获取第一组或全部数据
1	-	-	-	-	-	-	-	获取下一组数据

b) 数据域格式如下表所示：

表 17　数据域格式说明

数据域	长度（TLV 格式）	值	M/O
业务类型	1	明文	M

7.4.3　响应格式

返回对应标签（TAG）的数据，其数据内容为TLV格式，可同时存在多个标签（TAG）数据。

表 18 响应格式

数据域	长度（TLV 格式）	值	M/O
总长度	1-3	明文	M
$T_1L_1V_1$	XX	密文	M
MAC	4	使用会话密钥 macKey 对 总长度~（TLV1~TLVn）密文计算 MAC	M

参 考 文 献

待补充