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应用接口要求

Digital Identity Based On SIM Card

Application Interface Requirements For Dedicated Security Chips In Identity Authentication Devices

Verison 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：联通在线信息科技有限公司、中国联合网络通信有限公司、北京中盾安信科技发展有限公司、中移动金融科技有限公司、天翼电子商务有限公司、北京握奇数据股份有限公司、兴唐通信科技有限公司、楚天龙股份有限公司、上海复旦微电子集团股份有限公司、芯昇科技有限公司、北京中电华大电子设计有限责任公司、紫光同芯微电子有限公司、厦门中盾安信科技有限公司、北京中广瑞波科技股份有限公司。

起草人：梁斌、韩英晶、张林、程福兴、杨亮、曹德光、刘翔宇、王君珂、靳慧芳、王艳丽、黄炜耀、张新彬 、王性国、果艳红、梁栋、李金萍、蔡子凡、朱志高、李娟娜、范博贺、盖树天、于炜、高云鹏、林伟彬、周鹏。

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。

为了提高身份鉴别凭证使用过程中数据的规范性和安全性，指导用户进行身份鉴别设备软件开发、对接和使用，并定义身份鉴别设备与身份鉴别设备专用安全芯片之间交互过程中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 身份鉴别设备专用安全芯片应用接口要求

1 范围

本文件规定了身份鉴别设备专用安全芯片的应用接口要求。

本文件适用于身份鉴别设备专用安全芯片的应用接口的设计、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 32907—2016 信息安全技术 SM4分组密码算法

GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

3 术语、定义和缩略语

3.1 术语和定义

T/OIDAA XXX—XXXX界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语和符号适用于本文件。

SM2 SM2椭圆曲线公钥密码算法（public key cryptographic algorithm SM2 based on elliptic curves）

SM4 SM4分组密码算法（SM4 block cipher algorithm）

MAC 消息校验码（Message Authentication Code）

NFC 近场通信（Near Field communication）

SIM 用户识别卡（Subscriber Identity Module）

SEID 安全模块标识（Secure Element Identifier）

4 命令说明

4.1 命令格式

4.1.1 命令组成

表 1 命令组成

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

4.1.2 命令格式分类

表 2 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

4.2 响应格式

表 3 响应格式

数据	状态码	
DATA	SW1	SW2

DATA ：响应数据；
SW1、SW2：卡片执行命令的相应状态码。

5 应用命令

5.1 NFC INIT 命令

5.1.1 功能描述

此命令用于NFC外部认证初始化。

5.1.2 命令格式

表 4 NFC INIT 命令格式

数据	描述
CLA	80
INS	D3
P1	00
P2	00

LC	无
DATA	无
LE	00

5.1.3 响应格式

表 5 NFC INIT 响应数据

数据项	长度（TLV 格式）			值	M/O
随机数 RANDA	1	1	8	随机数 A，明文	M
身份鉴别设备专用安全芯片授权证书	1	2	169	身份鉴别设备专用安全芯片授权证书	M

表 6 NFC INIT 响应状态码

SW	描述
9000	执行成功
6985	当前状态不满足
6A86	P1P2 参数错误

5.2 NFC AUTH 命令

5.2.1 功能描述

此命令用于NFC外部认证。

5.2.2 命令格式

表 7 NFC AUTH 命令格式

数据	描述
CLA	80
INS	D4
P1	XX
P2	00
LC	数据域长度
DATA	数据域
LE	00

a) P1 参数格式描述：

表 8 NFC AUTH P1 参数格式

b8	b7	b6	b5	b4	b3	b2	b1	说明

0	-	-	-	-	-	-	-	非最后一条命令
1	-	-	-	-	-	-	-	最后一条命令

b) 数据域格式如下表所示：

表 9 NFC AUTH 数据域格式

数据项	长度（TLV 格式）			值	M/O
随机数 RANDB	1	1	104	使用身份鉴别设备专用安全芯片的公钥加密的随机数 B 密文，随机数不包含 TL	M
SIM 卡证书	1	2	147	明文	M
签名	1	1	64	SIM 卡私钥对随机数 RAND~SIM 卡证书的签名，签名值为原始签名数据	M

5.2.3 响应格式

表 10 NFC AUTH 响应数据

数据项	长度（TLV 格式）			值	M/O
签名	1	1	64	使用身份鉴别设备专用安全芯片的私钥对{RANDA|RANDB}的签名，签名值为原始签名数据	M

表 11 NFC AUTH 响应状态码

SW	描述
9000	认证成功
9304	签名无效
6700	LC 错误
6985	当前状态不满足
6A86	P1P2 参数错误
6A92	证书无效
6A80	数据错误

5.3 GET STATUS 命令

5.3.1 功能描述

此命令用于读取身份鉴别设备专用安全芯片的状态信息。

5.3.2 命令格式

表 12 GET STATUS 命令格式

数据	描述
CLA	80
INS	D5
P1	00
P2	00
LC	无
DATA	无
LE	00

5.3.3 响应格式

表 13 GET STATUS 响应数据

字段	长度	描述
STATE	1	状态值，默认为 0xFF，转为安全状态后为 0x01；非 TLV 格式。

表 14 GET STATUS 响应状态码

SW	描述
9000	执行成功

5.4 NFC DECRYPT 命令

5.4.1 功能描述

此命令用于解密使用NFC读取命令从SIM卡中读取的加密数据。

5.4.2 命令格式

表 15 NFC DECRYPT 命令格式

数据	描述
CLA	80
INS	D7
P1	XX
P2	00
LC	数据长度
DATA	数据域
LE	00

a) P1 参数格式：

表 16 NFC DECRYPT P1 参数格式

b8	b7	b6	b5	b4	b3	b2	b1	说明
0	0	-	-	-	-	-	-	非最后一条命令
1	0	-	-	-	-	-	-	最后一条命令
0	1	-	-	-	-	-	-	获取下一组数据

b) 数据域格式如下表所示：

表 17 NFC DECRYPT 数据域格式

数据域	长度（TLV 格式）			值	M/O
总长度	1-3			（TLV1~TLVn）数据密文~MAC 的总长度	M
$T_1L_1V_1$	XX			数据密文	M
$T_2L_2V_2$	XX				O
$T_3L_3V_3$	XX				O
……					O
$T_nL_nV_n$	XX				O
MAC	4			使用会话密钥 macKey 对 总长度~（TLV1~TLVn）密文计算 MAC 值	M
授权数据	1	1	16	授权数据，有身份鉴别凭证数据时必填。	C

5.4.3 响应格式

表 18 NFC DECRYPT 响应数据

数据域	长度（TLV 格式）	值	M/O
$T_1L_1V_1$	XX	数据 1，TLV 格式	M
$T_2L_2V_2$	XX	数据 2，TLV 格式	O
$T_3L_3V_3$	XX	数据 3，TLV 格式	O
……		……	O
$T_nL_nV_n$	XX	数据 n，TLV 格式	O

表 19 NFC DECRYPT 响应状态码

SW	描述
9000	执行成功
9302	MAC 无效
9305	授权数据不存在

6700	LC 错误
6985	当前状态不满足
6A86	P1P2 参数错误
6A80	数据错误
6310	存在后续数据等待获取，发送原命令（80D7400000）继续获取。

5.5 GET SEID 命令

5.5.1 功能描述

此命令用于从身份鉴别设备专用安全芯片中获取SEID，若身份鉴别设备专用安全芯片中不存在SEID，则报错。

5.5.2 命令格式

表 20 GET SEID 命令格式

数据	描述
CLA	80
INS	DA
P1	00
P2	00
LC	无
DATA	无
LE	00

5.5.3 响应格式

表 21 GET SEID 响应数据

数据域	长度	值	M/O
SEID	10	身份鉴别设备专用安全芯片ID（非TLV格式）	M

表 22 GET SEID 响应状态码

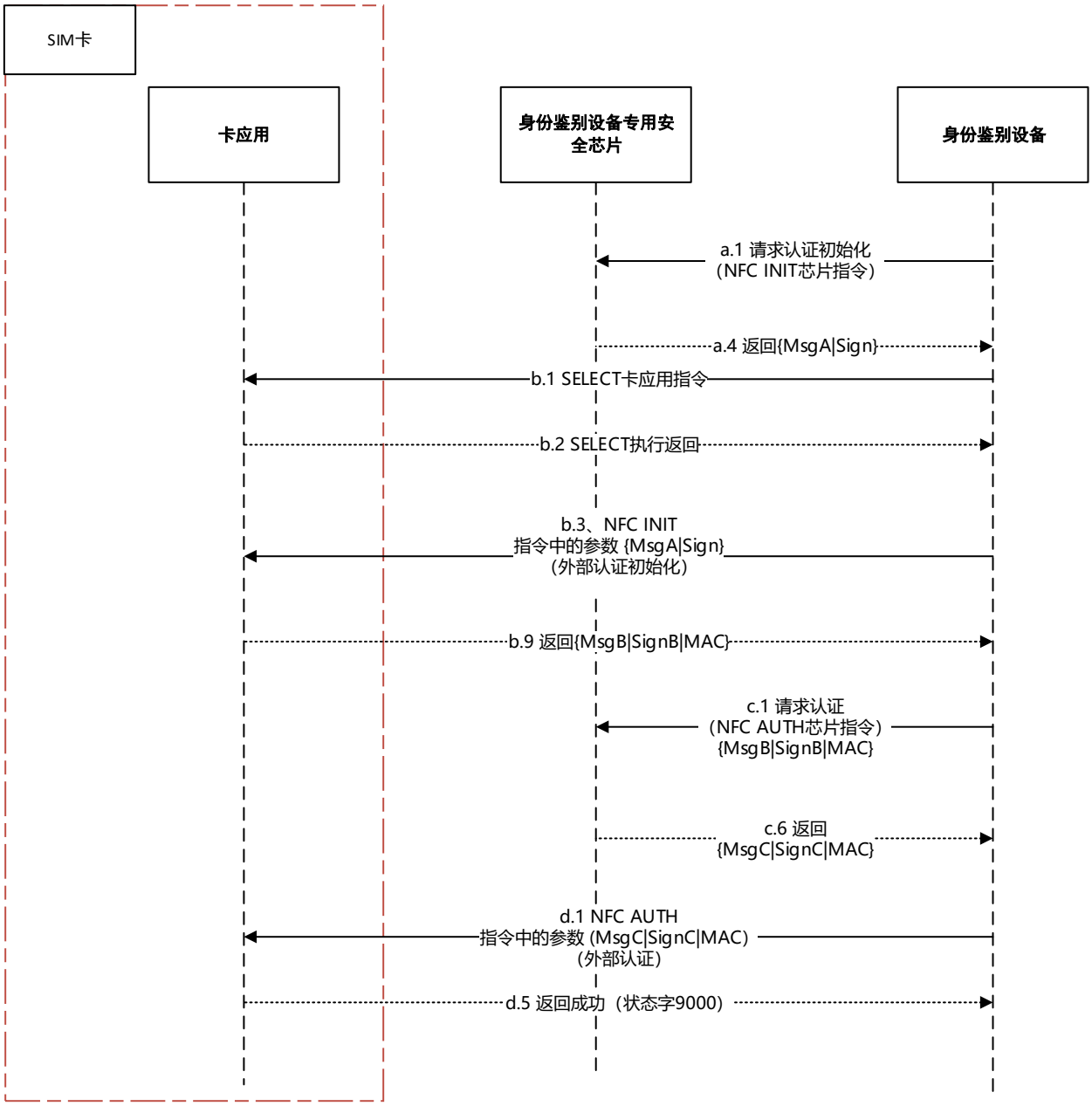
SW	描述
9000	执行成功
6A82	未找到文件

附 录 A

（资料性）

业务流程

A.1 NFC 外部认证流程



流程描述：

1 身份鉴别设备请求认证初始化

a) 身份鉴别设备请求身份鉴别设备专用安全芯片认证初始化，命令为 NFC INIT（芯片）；

b) 身份鉴别设备专用安全芯片返回{MsgA}。

2 身份鉴别设备与卡应用进行外部认证初始化。

a) 选择卡应用；

b) 身份鉴别设备发送 NFC INIT 命令到卡应用，进行外部认证初始化，参数为 MsgA；

c) 卡应用返回{MsgB（*RandB|SIM 卡证书）|SignB}。

3 身份鉴别设备请求外部认证

a) 身份鉴别设备请求身份鉴别设备专用安全芯片进行认证，命令为 NFC AUTH（芯片）；

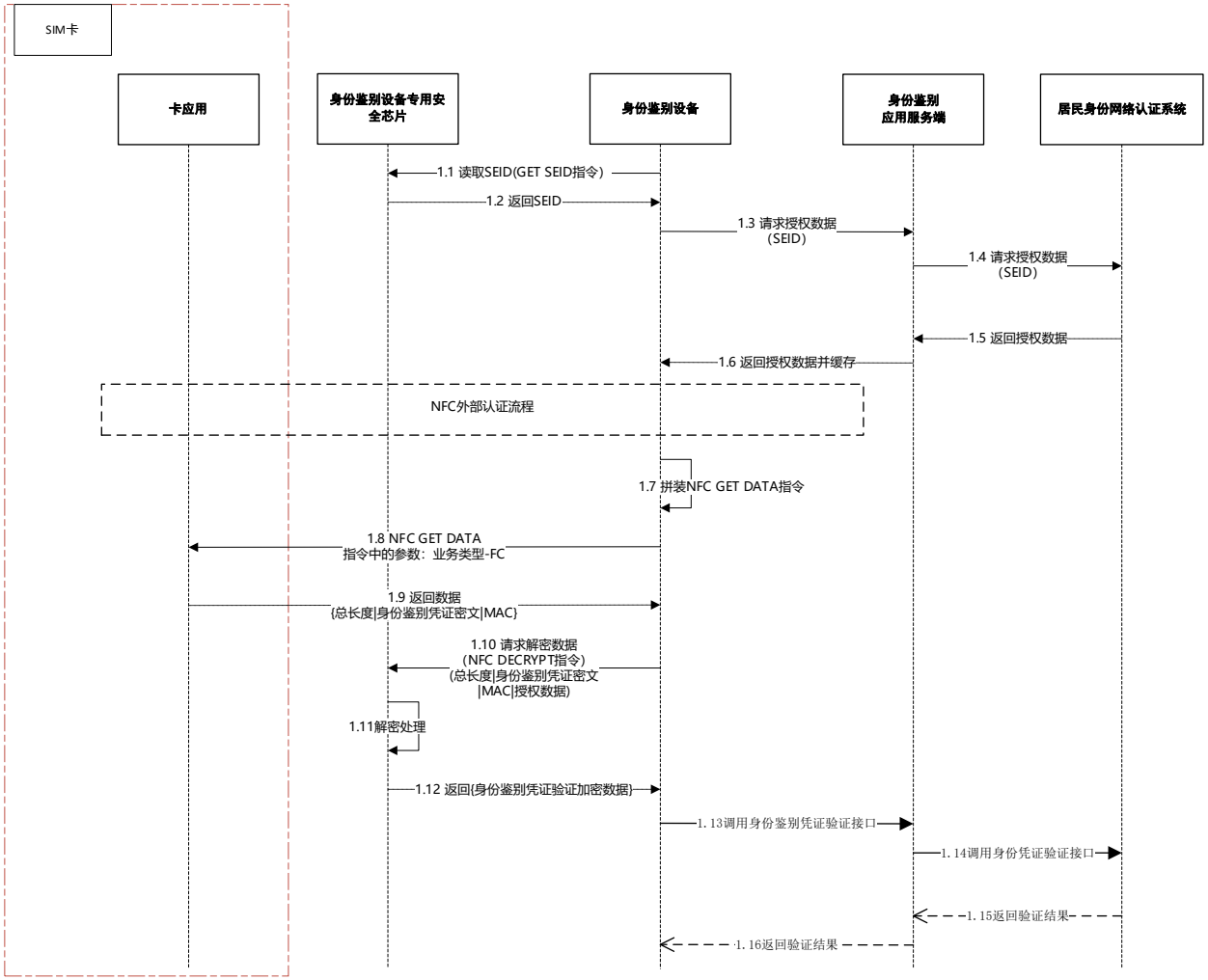
b) 身份鉴别设备专用安全芯片返回{SignC}给身份鉴别设备。

4 身份鉴别设备与卡应用进行外部认证

a) 身份鉴别设备发送 NFC AUTH 命令给卡应用进行外部认证，参数为{ SignC }；

b) 卡应用返回认证成功（状态字 9000），缓存认证状态。

A.2 NFC 线下读取身份鉴别凭证流程



流程描述：

身份鉴别设备使用身份鉴别设备专用安全芯片与卡应用完成外部认证流程。

1 身份鉴别设备请求身份鉴别应用服务端获取授权，身份鉴别应用服务端透传请求到居民身份网络认证系统，请求身份鉴别设备专用安全芯片读取身份鉴别凭证数据。

a) 身份鉴别设备读取身份鉴别设备专用安全芯片的 SEID；

b) 身份鉴别设备专用安全芯片返回 SEID；

c) 身份鉴别设备将 SEID 组装成请求数据到身份鉴别服务端请求授权；

d) 身份鉴别服务端通过向居民身份网络认证系统请求获取授权数据，参数为 SEID；

e) 居民身份网络认证系统返回业务授权数据，身份鉴别服务端将授权数据返回到身份鉴别设备；

f) 身份鉴别设备拼装 NFC GET DATA 命令，参数为业务类型（值为 FC）。

2 身份鉴别设备从卡应用读取数据。

a) 身份鉴别设备发送 NFC GET DATA 命令给卡应用；

b) 卡应用返回{总长度|身份鉴别凭证密文|MAC}给身份鉴别设备；

c) 身份鉴别设备请求身份鉴别设备专用安全芯片解密数据，命令为 NFC DECRYPT，参数为{总长度|身份鉴别凭证密文|MAC|授权数据}；

d) 身份鉴别设备专用安全芯片处理 NFC DECRYPT 命令流程，返回{身份鉴别凭证认证加密数据}给身份鉴别设备；

e) 身份鉴别设备将身份鉴别凭证上传到身份鉴别应用服务端进行验证，身份鉴别应用服务端将身份鉴别凭证透传到居民身份网络认证系统进行验证，并返回验证结果。

附 录 B

（规范性）

标签（TAG）定义

标签	长度(字节)	描述
D1	10	SEID
D4	16	授权数据
D5	XX	身份鉴别凭证验证加密数据
D7	192	证书信息密文
42	8	随机数
83	64	签名值，原始签名数据
84	104	随机数密文
91	147	SIM 卡证书
93	153	身份鉴别设备专用安全芯片授权证书
94	147	居民身份网络认证系统证书
9B	147	身份鉴别设备专用安全芯片授权根证书
CC	变长	数据密文

附 录 C

（规范性）

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

参 考 文 献