ICS 33.050
CCS M 30

团　体　标　准

T/TAF 251—2024

基于SIM卡的数字身份认证技术要求

Technical requirements for SIM card based digital identity authentication

2024-11-01 发布　　2024-11-01 实施

电信终端产业协会　发布

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　基于 SIM 卡的数字身份认证技术架构 2
6　安装在 SIM 卡上的数字身份应用 3
6.1　应用架构 3
6.2　应用状态管理 4
7　用户使用的数字身份业务状态 4
7.1　概述 4
7.2　业务申领 5
7.3　业务开通 6
7.4　业务暂停 8
8　SIM 卡要求 9
8.1　硬件要求 9
8.2　密钥管理和密码算法要求 9
8.3　应用要求 10
9　终端要求 10
9.1　手机终端要求 10
9.2　数字身份识别设备要求 10
10　平台要求 11
10.1　数字身份业务管理平台要求 11
10.2　数字身份应用管理平台要求 11
10.3　数字身份认证服务平台要求 11
附录 A（资料性）　基于 SIM 卡的数字身份认证场景示例 12
A.1　概述 12
A.2　方式一：通过手机终端 APP 完成数字身份认证 12
A.3　方式二：通过数字身份识别设备完成数字身份认证 13

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。

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中移动金融科技有限公司、联通在线信息科技有限公司、中国联合网络通信有限公司、中国信息通信研究院、天翼电信终端有限公司、郑州信大捷安信息技术股份有限公司、国民认证科技（重庆）有限公司、北京一砂信息技术有限公司。

本文件主要起草人：董扬、王君珂、果艳红、庄怀宇、谷博、梁斌、袁琦、唐欢、王昊、程福兴、张林、杨亮、张宏星、刘萧萧、闫彦、徐从德、李俊、刘献伦、张楚、张盛毅、幸宇、崇静、阎国臣、毕亚超、李鑫、彭金辉。

引　言

SIM卡是连接运营商服务和用户的关键入口，是运营商与用户之间的重要触点。新一代SIM卡支持多种通信协议、多安全算法和功能丰富的API，具有自主可控、高安全性、高可靠性等特点，在功能上已由单一的通信载体升级为IT安全服务工具。

SIM卡作为高安全性的硬件安全模块，是数字身份的理想载体，SIM卡内集成数字身份可实现自然人、手机号、SIM卡、网络身份凭证等“人号卡证”四统一。其应用方式除通过手机终端APP读取SIM卡内身份信息进行认证外，还可通过NFC方式有效支持离线、快速通行类应用，可为用户提供安全便捷的数字身份存储、加密和互联服务。

本文件围绕线上、线下各类场景下的身份认证需求，对以SIM卡为“可信数字身份”信任根，集成数字身份基础能力的SIM数字身份业务提出通用的安全技术要求，可用于指导相关企业设计、开发和运营基于SIM卡的数字身份产品，推动线上线下数字身份应用深度融合。

基于SIM卡的数字身份认证技术要求

1 范围

本文件规定了基于SIM卡的数字身份认证技术要求，包括技术架构、安装在SIM卡上的数字身份应用、用户使用的数字身份业务状态、SIM卡要求、终端要求和平台要求。

本文件适用于基于SIM卡的数字身份认证技术的设计、开发和运营等。

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 25069—2022 信息安全技术 术语

ETSI TS 102 223（所有部分） 智能卡；卡应用工具包(CAT)（Smart Cards; Card Application Toolkit (CAT)）

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

数字身份 digital identity

主体在互联网中的身份表示，关联了与该主体相关的属性信息，通常由一个账户标识其唯一性。

3.2

BIP协议 Bearer Independent Protocol

BIP协议是承载无关协议，是ETSI TS 102 223中提出的一种面向连接的传输协议。协议支持GSM、CDMA、UMTS、NG-RAN 等移动网络，允许SIM卡通过终端与服务器建立基于IP的数据连接，SIM卡在信道建立的时候通知终端可选择的信息承载方式，SIM卡通常支持基于BIP的HTTPS协议。终端允许SIM卡和服务器在该信道上透明地交换数据，应用中具体承载的数据传输协议与BIP通道无关。

4 缩略语

下列缩略语适用于本文件。

AES:高级加密标准算法（Advanced Encryption Standard algorithm）

APP：应用程序（Application）

BIP：承载无关的协议（Bearer Independent Protocol）

CDMA：码分多址（Code Division Multiple Access）

COS：用户卡操作系统（Chip Operation System）
GSM：全球移动通信系统（Global System for Mobile communications）
HTTPS：安全超文本传输协议（HyperText Transfer Protocol Secure）
IP：互联网协议（Internet Protocol）
NG-RAN：下一代无线接入网（Next Generation Radio Access Network）
NFC：近场通信（Near Field Communication）
PIN：个人标识符（Personal Identification Number）
RSA：RSA加密算法（Rivest-Shamir-Adleman algorithm）
SDK：软件开发工具包（Software Development Kit）
SHA-256：安全散列算法256（Secure Hash Algorithm 256）
SIM：用户识别卡（Subscriber Identity Module）
SWP：单线协议（Single Wire Protocol）
UMTS：通用移动通信系统（Universal Mobile Telecommunication System）
WLAN：无线局域网（Wireless Local Area Networks）

5 基于SIM卡的数字身份认证技术架构

基于SIM卡的数字身份认证技术架构见图1，包括数字身份业务管理平台、数字身份应用管理平台、数字身份认证服务平台、装载数字身份APP的手机终端、装载数字身份应用的SIM卡及数字身份识别设备六个部分。

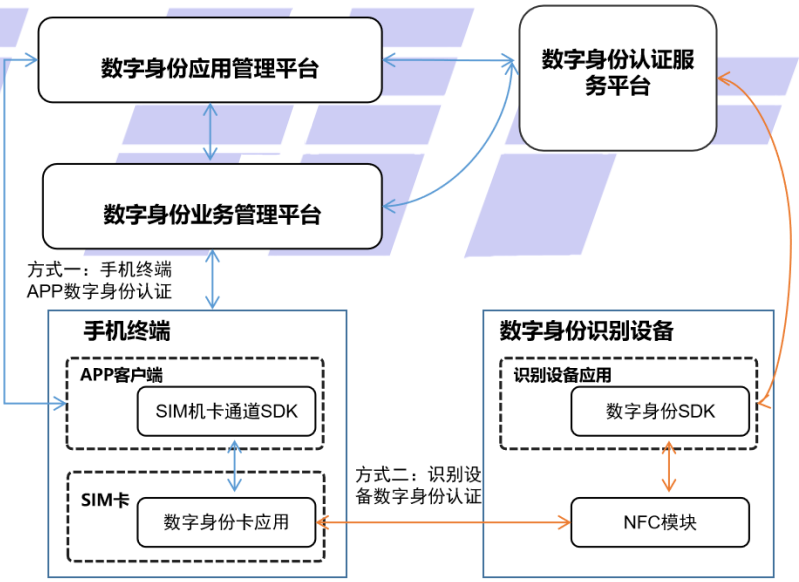


图1 基于SIM卡的数字身份认证技术架构

基于SIM卡的数字身份认证技术架构各部分功能如下：

a) 数字身份业务管理平台是数字身份认证业务的系统平台，完成用户身份数据管理、身份认证业务指令处理并对接数字身份认证服务平台，以完成数字身份认证；
b) 数字身份应用管理平台是SIM卡的应用管理及能力开放系统平台，负责完成对SIM卡上存储空间的管理，并提供数字身份应用发布、更新及下载等服务；
c) 数字身份认证服务平台负责处理数字身份业务管理平台发送的认证请求，并返回认证结果或相

关信息；

d) 装载数字身份 APP 的手机终端：手机终端具备 BIP、机卡通信等基础能力，并安装数字身份 APP，APP 集成 SIM 卡机卡通道的 SDK，通过机卡通道或 BIP 通道完成数字身份认证操作和业务生命周期管理、个人数字身份信息读取等操作，通过移动网络或 WLAN 网络连接数字身份业务管理平台，完成数字身份认证；

e) 装载数字身份应用的SIM卡：装载数字身份应用，存储用户个人的数字身份信息和敏感数据，具备安全存储、安全计算、安全通信、安全管理等能力；

f) 数字身份设别设备：集成数字身份 SDK，具备本地认证或在线连接数字身份业务管理平台进行认证的能力，具备 NFC 通信能力。对于不具备专用安全模组的数字身份识别设备，使用 NFC 通道读取 SIM 卡上的数字身份信息，使用移动网络或 WLAN 网络连接数字身份认证服务平台完成数字身份认证，并将认证结果和数字身份信息返回给数字身份识别设备；对于具备专用安全模组的数字身份识别设备，使用 NFC 通道读取 SIM 卡上的数字身份信息，直接在本地完成数字身份认证。

用户使用手机终端APP通过在线连接的方式与数字身份业务管理平台建立连接，完成数字身份申领，申领成功后将个人数字身份写入SIM卡并完成数字身份业务开通。数字身份业务开通后，用户可使用SIM卡上的数字身份完成身份认证业务。数字身份认证包括手机终端APP认证和数字身份设别设备认证两种方式，根据认证的安全级别和要求不同，可进行用户实人认证和实名认证，认证流程详见附录 A。

6 安装在 SIM 卡上的数字身份应用

6.1 应用架构

安装在SIM卡上的数字身份应用包括通用数据管理、个人身份信息管理、状态管理和版本管理等功能模块，各个模块功能说明如下：

a) 通用数据管理模块主要用于密钥及证书的管理，包括：应用序列号、管理密钥、业务密钥、业务管理证书和 SIM 卡证书等；

b) 个人身份信息管理模块用于管理身份信息及电子证照业务相关的数据和业务指令处理，包括身份信息写入、身份信息读取、身份信息更新、身份信息删除；

c) 状态管理模块主要包括应用状态机管理、业务状态管理和业务指令控制；

d) 版本管理模块用于应用管理，包括应用版本和应用状态管理。

安装在SIM卡上的数字身份应用架构见图2。

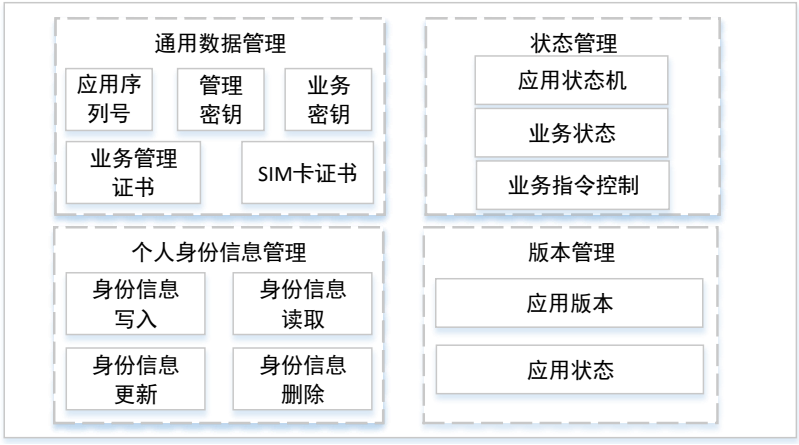


图2 安装在SIM卡上的数字身份应用架构

6.2 应用状态管理

安装在SIM卡上的数字身份应用状态流程见图3。

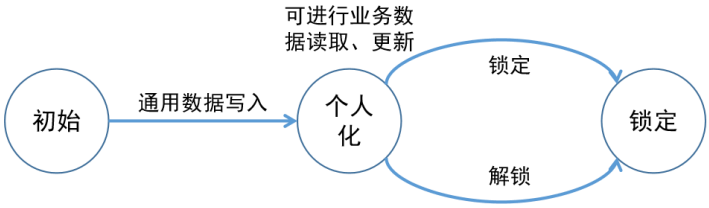


图 3 安装在 SIM 卡上的数字身份应用状态流程

安装在SIM卡上的数字身份应用状态流程说明具体如下：

a) 当用户写入应用序列号和管理密钥后，应用业务状态设置为“个人化”；

b) “个人化”状态可以进行各业务数据的读取和更新等操作，卡片安全受到威胁时可对应用进行锁定；

c) 应用解锁后，应用状态将从“锁定”切换为“个人化”。

安装在SIM卡上的数字身份应用在不同状态下可进行的操作见表1。

表1 数字身份应用状态表

状态	描述	后续状态
初始	数字身份应用安装完成，可写入应用序列号和管理密钥	个人化
个人化	可进行业务数据的读取和更新	锁定
锁定	不能进行任何业务数据操作	个人化

7 用户使用的数字身份业务状态

7.1 概述

用户使用的数字身份业务状态包括：业务申领完成、业务开通完成、业务暂停完成三个状态，数字身份应用下载并完成个人化后，业务状态为申领完成状态，管理流程见图4。

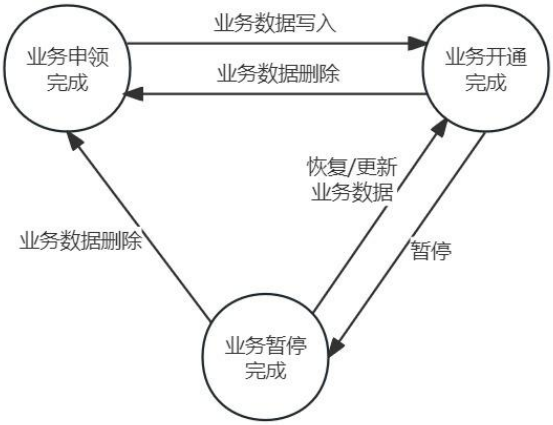


图4 用户使用的数字身份业务状态管理流程

用户使用的数字身份业务所处状态描述见表2。

表2　业务状态表

状态	描述	后续状态
业务申领完成	数字身份应用下载并完成个人化后，业务状态为申领完成状态； 在开通完成状态/暂停完成状态下删除全部业务数据后，业务状态更新为申领完成状态	业务开通完成
业务开通完成	在申领完成状态写入业务数据后，业务状态更新为开通完成状态； 在暂停完成状态恢复/更新业务数据后，业务状态更新为开通完成状态	业务申领完成、业务暂停完成
业务暂停完成	在开通完成状态下，完成业务暂停操作后，业务状态更新为暂停完成状态	业务开通完成、业务申领完成

7.2　业务申领

7.2.1　通过 BIP 通道申领数字身份

通过BIP通道申领数字身份流程见图5。

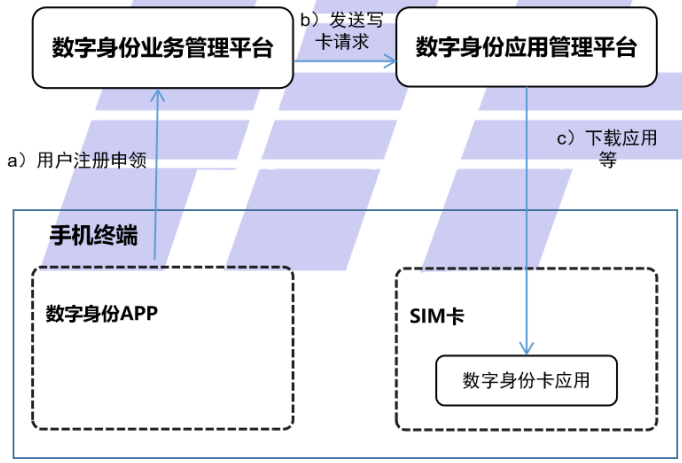


图5　通过BIP通道完成数字身份申领

用户通过BIP通道申领数字身份，此过程将同步完成SIM卡上的数字身份应用下载、安装及初始信息写入，具体步骤如下：

a）　用户通过手机终端数字身份 APP 发起数字身份认证业务注册申领；

b）　数字身份业务管理平台收到用户申请后，向数字身份应用管理平台发送应用下载请求；

c）　数字身份应用管理平台与 SIM 卡建立 BIP 通道，并通过 BIP 通道下发数字身份应用数据，SIM 卡完成数字身份应用下载和安装后，将安装在 SIM 卡上的数字身份应用状态设置为初始状态，数字身份业务管理平台通过数字身份应用管理平台向 SIM 卡中写入应用序列号、初始管理密钥、业务密钥和相关证书后，安装在 SIM 卡上的数字身份应用进入个人化状态，用户使用的数字身份业务状态同步切换到业务申领完成状态。

7.2.2 通过机卡通道申领数字身份

通过机卡通道申领数字身份流程见图6。

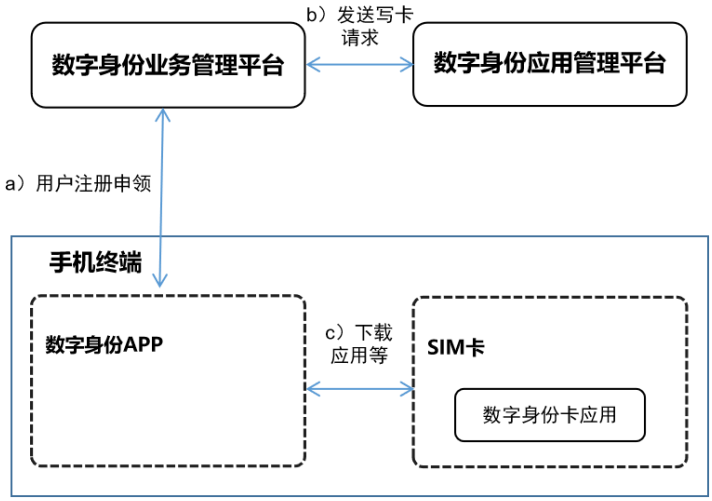


图6 通过机卡通道完成数字身份申领

用户通过机卡通道申领数字身份，此过程将同步完成SIM卡上的数字身份应用下载、安装及初始信息写入，具体步骤如下：

a) 用户通过手机终端数字身份 APP 发起数字身份认证业务注册申领；

b) 数字身份业务管理平台收到用户申请后，向数字身份应用管理平台发送数字身份应用下载请求，数字身份应用管理平台将数字身份应用及数据返回数字身份业务管理平台；

c) 数字身份业务管理平台借助数字身份 APP，通过机卡通道下发数字身份应用数据，SIM 卡完成数字身份应用下载和安装后，将安装在 SIM 卡上的数字身份应用状态设置为初始状态，数字身份业务管理平台向 SIM 卡中写入应用序列号、初始管理密钥、业务密钥和相关证书后，安装在 SIM 卡上的数字身份应用进入个人化状态，用户使用的数字身份业务状态同步切换到申领完成状态。

7.3 业务开通

7.3.1 通过 BIP 通道开通数字身份

通过BIP通道开通数字身份流程见图7。

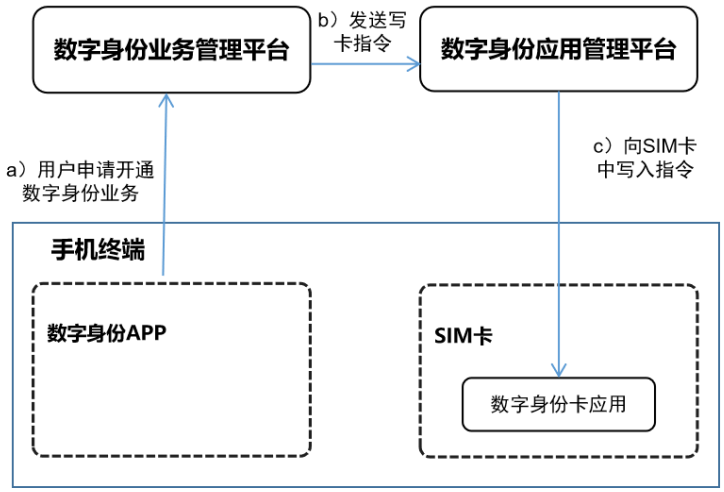


图7　通过BIP通道完成数字身份开通

用户申领数字身份后，可通过手机终端数字身份APP发起开通业务流程完成业务开通。通过BIP通道完成数字身份开通流程，具体步骤如下：

a）　用户通过手机终端数字身份 APP 发起数字身份认证业务开通申请；

b）　数字身份业务管理平台收到用户开通申请后，组织业务开通数据指令，发送给数字身份应用管理平台；

c）　数字身份应用管理平台与 SIM 卡建立 BIP 通道,并下发业务开通数据指令，安装在 SIM 卡上的数字身份应用收到指令后完成数据更新操作，并将当前用户使用的数字身份业务状态更新为开通完成状态。

7.3.2　通过机卡通道开通数字身份

通过机卡通道开通数字身份流程见图8。

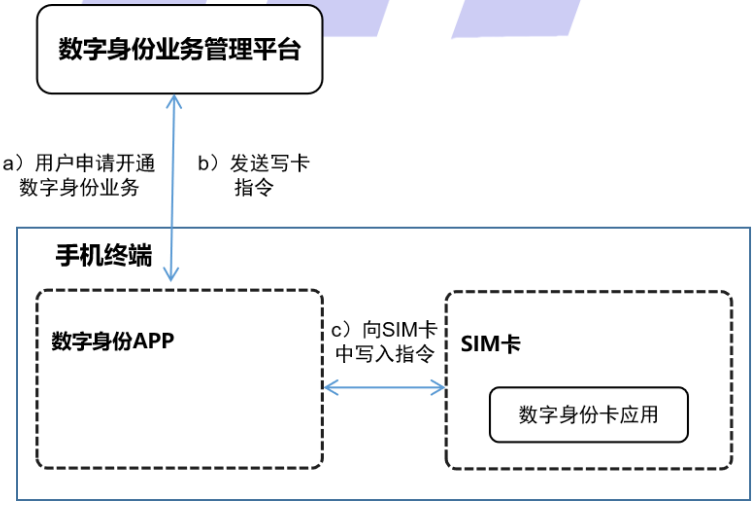


图8　通过机卡通道完成数字身份开通

通过机卡通道完成数字身份开通时只需要访问数字身份业务管理平台，具体步骤如下：

a）　用户通过数字身份认证手机终端数字身份 APP 发起数字身份认证业务开通申请；

b） 数字身份业务管理平台收到用户开通申请后，组织业务开通数据指令，下发给手机终端数字身份 APP；

c） 手机终端数字身份 APP 通过机卡通道向 SIM 卡发送开通数据指令，安装在 SIM 卡上的数字身份应用收到指令后完成数据更新操作，并将当前用户使用的数字身份业务状态更新为开通完成状态。

7.4 业务暂停

7.4.1 通过 BIP 通道暂停数字身份

通过BIP通道暂停数字身份流程见图9。

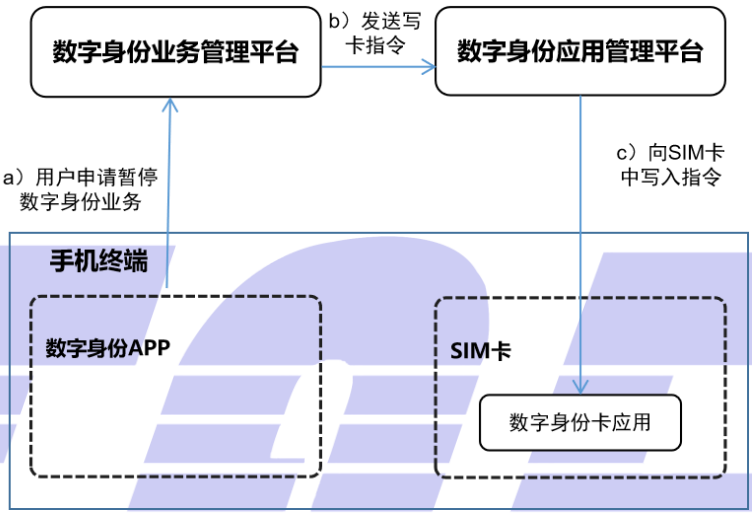


图9 通过BIP通道完成数字身份业务暂停

用户开通数字身份后，可通过手机终端数字身份APP主动申请数字身份业务暂停，当数字身份业务管理平台判定用户数字身份处于被攻击、盗用等不安全状态时，数字身份业务管理平台也可主动发起业务暂停流程，具体步骤如下：

a） 用户通过手机终端数字身份 APP 发起数字身份认证业务暂停申请；

b） 数字身份业务管理平台组织业务暂停数据指令，发送给数字身份应用管理平台（数字身份业务管理平台主动发起业务暂停时流程从此步开始）；

c） 应用平台与 SIM 卡建立 BIP 通道，并下发相关业务指令，安装在 SIM 卡上的数字身份应用收到指令后完成数据更新操作，并将当前业务状态更新为暂停完成状态，业务暂停后，SIM 卡上的所有数字身份相关的功能均不能使用。

7.4.2 通过机卡通道暂停数字身份

通过机卡通道暂停数字身份流程见图10。

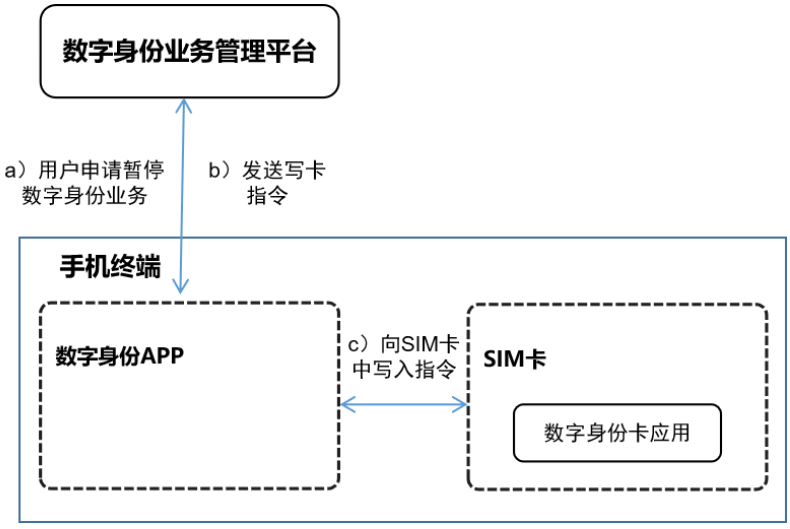


图10　通过机卡通道完成数字身份业务暂停

通过机卡通道完成数字身份暂停时只需要与数字身份业务管理平台进行交互，，具体步骤如下：

a）　用户通过手机终端数字身份 APP 发起数字身份认证业务暂停申请；

b）　数字身份业务管理平台组织业务暂停数据指令，下发给手机终端数字身份 APP；（数字身份业务管理平台主动发起业务暂停时流程从此步开始）；

c）　手机终端数字身份 APP 通过机卡通道向 SIM 卡发送暂停数据指令，安装在 SIM 卡上的数字身份应用收到指令后完成数据更新操作，并将当前业务状态更新为暂停完成状态，业务暂停后，SIM 卡上的所有数字身份相关的功能均不能使用。

8　SIM 卡要求

8.1　硬件要求

硬件要求如下：

a）　SIM 卡通信接口要求如下：

1）　SIM 卡应支持 ISO7816 接口；

2）　SIM卡应支持SWP接口。

b）　SIM 卡内存要求如下：

1）　SIM 卡非易失性存储应可擦写至少 10 万次，数据可至少保持 10 年；

2）　SIM卡易失性存储应至少达到2 kbytes。

c）　SIM 卡芯片应至少满足以下一种以上安全认证要求：

1）　满足GB/T 18336.3-2015规定的评估保障级4（EAL4）以上（含）或ISO/IEC 15408规定的的EAL4+以上（含）要求；

2）　满足GM/T 0008 安全等级二级以上（含）要求；

3）　符合银联卡芯片安全认证或EMVCo安全认证。

8.2　密钥管理和密码算法要求

密钥管理和密码算法要求如下：

a）　密钥类型：

1） SIM 卡中应至少有一组管理密钥，用于获取访问权限和安全通道的建立，该密钥可更新；
2） SIM 卡中应至少有一组业务密钥，用于保证业务数据交互过程中的安全性和有效性，该密钥可更新。

b） 密钥生成
1） SIM卡应支持密钥生成功能。
2） SIM卡中使用的对称密钥应保证唯一性，不同SIM卡配置不同密钥，密钥保存在SIM卡中；
3） SIM卡中使用的非对称密钥由SIM卡生成，私钥不能导出SIM卡。

c） 密钥写入：
1） SIM卡中的密钥可通过机卡通道或BIP通道写入；
2） SIM卡中的密钥写入时，应对待写入密钥数据进行加密。

d） 密钥使用：
1） SIM卡应支持随机分散方式。由SIM卡生成的随机数作为分散因子，使用分散因子采用对称算法对主密钥进行一级分散，得到过程密钥；
2） SIM卡应支持动态交换方式。数字身份认证服务平台或数字身份识别设备和SIM卡首先交换各自公钥证书，其次双方各自生成业务密钥，再使用对方公钥分别完成业务密钥加密，最后双方完成密钥交换，解密后双方业务密钥合成统一过程密钥。

e） 密钥销毁：
1） 当数字身份应用暂停时，SIM卡删除当前使用的业务密钥，并无法读取数字身份信息，重新恢复到开通状态时，需要重新申请业务密钥；
2） 当数字身份应用删除时，必须删除与安装在SIM卡上的数字身份应用关联的所有业务密钥。

f） 密码算法：
1） SIM卡应支持对称算法的数据加/解密功能，包括AES和SM4等；
2） SIM卡应支持非对称算法的数据加/解密功能，包括RSA2048、SM2等；
3） SIM卡应支持数字签名及验签功能，包括SHA-256、SM3等。

8.3 应用要求

应用要求如下：

a） SIM 卡应支持数字身份应用在线及离线下载、安装、删除功能；
b） SIM 卡应支持数字身份应用下载、安装、删除过程异常处理机制；
c） SIM 卡应支持安全存储区授权读、写、空间分配、空间释放等功能；
d） SIM 卡应支持用户鉴权功能，可采用 PIN、生物特征识别等方式；
e） 如异常掉电事件发生时，SIM 卡应保证非易失性存储区内的数据不会丢失。

9 终端要求

9.1 手机终端要求

手机终端要求如下：

a） 手机终端应支持 BIP 通讯协议，SIM 卡可通过手机终端与数字身份应用管理平台建立 BIP 通道；
b） 手机终端宜支持 NFC 功能，实现数字身份识别设备和 SIM 卡之间的数据交互；
c） 手机终端数字身份 APP 应集成 SIM 卡机卡通道的 SDK，可采用本地或在线方式完成数字身份认证、业务生命周期管理和个人数字身份信息读取操作。

9.2 数字身份识别设备要求

数字身份识别设备要求如下：

a) 数字身份识别设备应具备 NFC 通信能力，用于与 SIM 卡通过 NFC 进行数据交互；
b) 数字身份识别设备应具备联网能力，支持将数据传输至数字身份业务管理平台核验；
c) 数字身份识别设备可集成安全模组，用于解密 SIM 卡上的身份信息进行本地核验。

10 平台要求

10.1 数字身份业务管理平台要求

数字身份业务管理平台要求如下：

a) 数字身份业务管理平台应具备与数字身份应用管理平台和数字身份认证服务平台建立安全连接的能力；
b) 数字身份业务管理平台应具备生成业务数据的能力，并对业务数据进行管理；
c) 数字身份业务管理平台应具备业务数据解析及异常处理能力；
d) 数字身份业务管理平台应支持 SM2、SM3、SM4 等安全算法，并具备业务数据加解密及完整性校验能力。

10.2 数字身份应用管理平台要求

数字身份应用管理平台要求如下：

a) 数字身份应用管理平台应具备与 SIM 卡建立 BIP 链接的能力；
b) 数字身份应用管理平台应具备 BIP 通道数据收发及业务数据解析能力；
c) 数字身份应用管理平台应支持 SIM 卡应用下载、安装、删除、密钥管理等 SIM 卡片上内容管理功能；
d) 数字身份应用管理平台应具备与数字身份业务管理平台和数字身份认证服务平台建立安全连接的能力；
e) 数字身份应用管理平台应支持 SM2、SM3、SM4 等安全算法，并具备业务数据加解密及完整性校验能力。

10.3 数字身份认证服务平台要求

数字身份认证服务平台要求如下：

a) 数字身份认证服务平台应具备与数字身份应用管理平台、数字身份业务管理平台建立安全连接的能力；
b) 数字身份认证服务平台应支持 SM2、SM3、SM4 等安全算法，并具备业务数据加解密及完整性校验。

附 录 A
（资料性）
基于 SIM 卡的数字身份认证场景示例

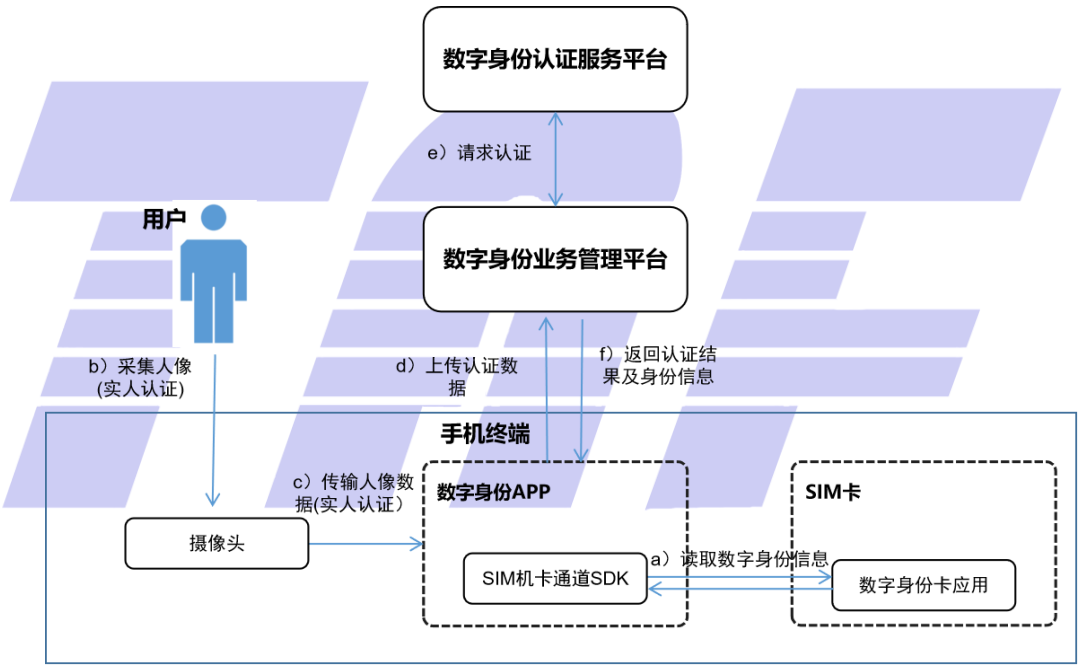
A.1 概述

数字身份业务开通后，用户可使用SIM卡上的数字身份应用完成身份认证业务。数字身份认证包括手机终端数字身份APP认证和数字身份识别设备认证两种方式，根据认证的安全级别和要求不同，可进行用户实人认证和实名认证，以下针对手机终端数字身份APP认证和数字身份识别设备认证两种认证方式进行详细描述。

A.2 方式一：通过手机终端 APP 完成数字身份认证

A.2.1 手机终端 APP 通过机卡通道进行在线认证

手机终端 APP 通过机卡通道进行在线认证流程见图 A.1。



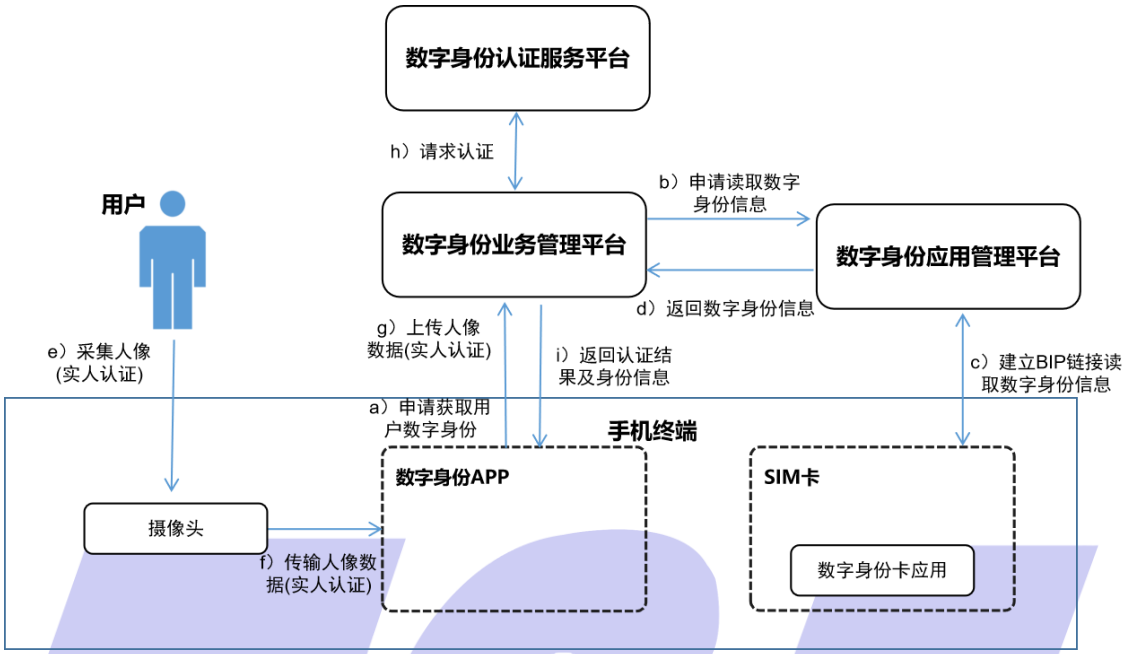
图A.1 手机终端APP机卡通道进行在线认证

手机终端数字身份APP机卡通道进行在线认证，通过手机终端数字身份APP读取SIM卡上的数字身份信息，并连接数字身份业务管理平台，完成数字身份认证，具体步骤如下：

a） 手机终端数字身份 APP 通过 SIM 机卡通道 SDK 调用机卡通道，通过机卡通道读取 SIM 卡中的数字身份信息；
b） 通过手机摄像头采集用户人像进行实人认证（非实人认证时跳过 b）、c）步）；
c） 手机摄像头将采集的人像数据传输给手机终端数字身份 APP；
d） 手机终端数字身份 APP 将用户认证数据上传至数字身份业务管理平台；
e） 数字身份业务管理平台向数字身份认证服务平台请求认证，并获取认证结果；
f） 数字身份业务管理平台将认证结果和实人信息返回给手机终端数字身份 APP。

A.2.2 手机终端 APP 通过 BIP 通道进行在线认证

手机终端 APP 通过 BIP 通道进行在线认证流程见图 A.2。



图A.2 手机终端APP通过BIP通道进行在线认证

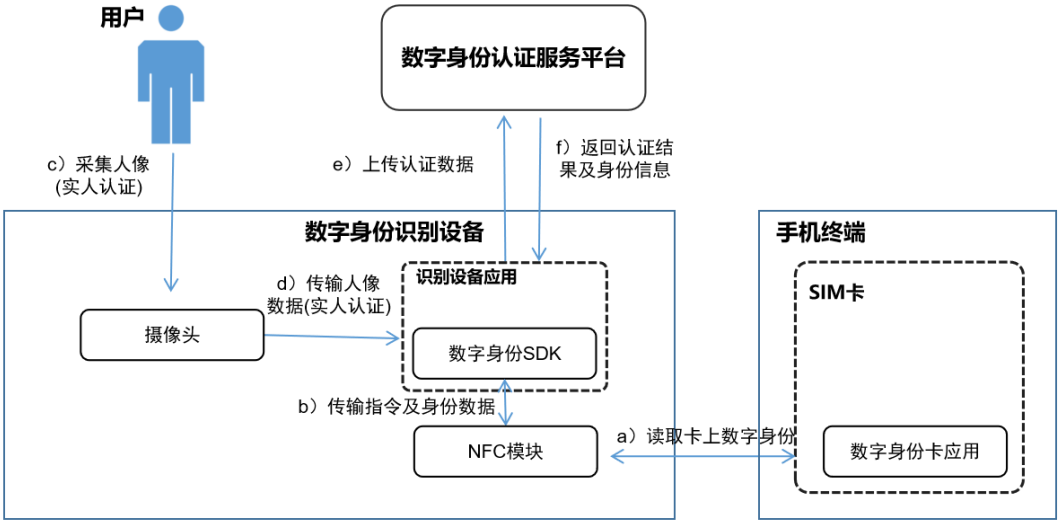
手机终端数字身份APP通过BIP通道进行在线认证，由数字身份应用管理平台通过BIP通道读取SIM卡上的数字身份信息，并连接数字身份业务管理平台，完成数字身份认证，具体步骤如下：

a） 手机终端数字身份 APP 连接数字身份业务管理平台，申请获取用户数字身份信息；
b） 数字身份业务管理平台连接数字身份应用管理平台，申请读取 SIM 卡上的数字身份信息；
c） 数字身份应用管理平台与 SIM 卡建立 BIP 链接，并读取 SIM 卡中的数字身份信息；
d） 数字身份应用管理平台向数字身份业务管理平台返回 SIM 卡中的数字身份信息；
e） 通过手机摄像头采集用户人像进行实人认证（非实人认证时跳过 e）、f）、g）步）；
f） 手机摄像头将采集的人像数据传输给手机终端数字身份 APP；
g） 手机终端数字身份 APP 将用户人像数据上传至数字身份业务管理平台进行实人核验；
h） 数字身份业务管理平台向数字身份认证服务平台请求认证，并获取认证结果；
i） 数字身份业务管理平台将认证结果及身份信息返回给手机终端数字身份 APP。

A.3 方式二：通过数字身份识别设备完成数字身份认证

A.3.1 数字身份识别设备进行在线身份认证

数字身份识别设备进行在线身份认证流程见图 A.3。



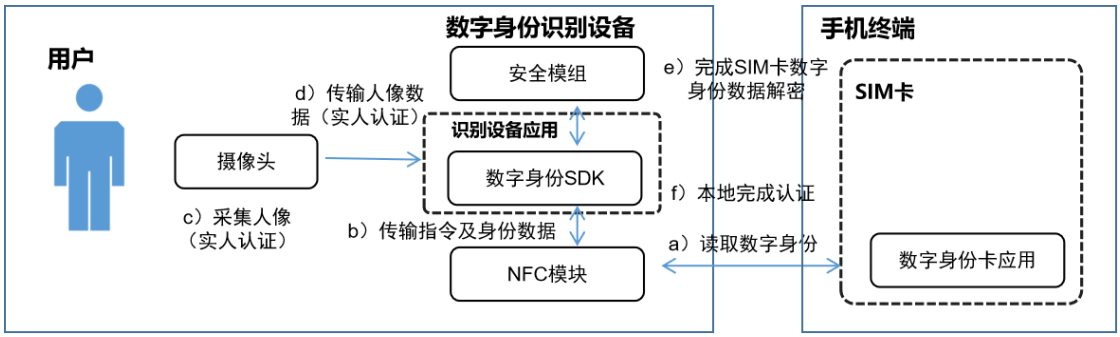
图A.3　数字身份识别设备进行在线身份认证

数字身份识别设备进行在线身份认证，由数字身份识别设备通过NFC读取SIM卡上的数字身份信息，并连接数字身份认证服务平台完成数字身份认证，具体步骤如下：

a）　数字身份识别设备调用 NFC 模块，读取 SIM 卡上的数字身份信息；
b）　NFC 模块读取的数字身份信息，传输给数字身份识别设备；
c）　通过数字身份识别设备自身摄像头采集用户人像进行实人认证（非实人认证时跳过 c）、d）步）；
d）　数字身份识别设备摄像头将采集的人像数据传输给数字身份识别设备；
e）　数字身份识别设备将用户认证数据上传至数字身份认证服务平台进行认证；
f）　数字身份认证服务平台将认证结果和用户身份信息返回给数字身份识别设备。

A.3.2　数字身份识别设备进行本地身份认证

数字身份识别设备进行本地身份认证流程见图 A.4。



图A.4　数字身份识别设备进行本地身份认证

数字身份识别设备进行本地身份认证，由数字身份识别设备通过NFC读取SIM卡上的数字身份信息，由数字身份识别设备自身的安全模组将读取的数字身份信息解密并在本地进行核验，具体步骤如下：

a）　数字身份识别设备调用 NFC 模块读取 SIM 卡上的数字身份信息及人像信息；

b) NFC 模块将读取的数字身份信息及人像信息传输给数字身份识别设备；
c) 通过数字身份识别设备自身摄像头采集用户人像进行实人认证（非实人认证时跳过 c）、d）步）；
d) 数字身份识别设备摄像头将采集的人像数据传输给终端应用；
e) 数字身份识别设备调用安全模组解密读取到的数字身份信息；
f) 数字身份识别设备完成数字身份信息核验及认证。

电信终端产业协会团体标准

基于 SIM 卡的数字身份认证技术要求

T/TAF 251—2024

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn