ICS 67.140.10
CCS X 55

团　　体　　标　　准

T/OIDAA XXX—XXXX

基于SIM卡的数字身份 身份鉴别设备技术要求

SIM-based Digital Identity Technical Requirements for Authentication Devices

XXXX-XX-XX 发布　　XXXX-XX-XX

中关村安信网络身份认证产业联盟　　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 概述 1
5 技术要求 2
6 安全要求 4
参考文献 6

图 1 身份鉴别设备通用技术架构 2

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、熵基科技股份有限公司、兴唐通信科技有限公司、前海联大（深圳）技术有限公司、厦门中盾安信科技有限公司、天翼电子商务有限公司、全民认证科技（杭州）有限公司、北京中广瑞波科技股份有限公司、北京中电华大电子设计有限责任公司、芯昇科技有限公司。

起草人：王性国、果艳红、王昊、庄怀宇、唐欢、管毅、刘金地 、梁斌、张林、吴朕阳、蔡子凡、许雪姣、林尧禹、温扬睿 、梁栋、霍红文、周鹏、张硕、范博贺。

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。

为统一规范基于SIM卡的数字身份身份鉴别设备提供身份鉴别凭证读取、验证的能力，并指导身份鉴别设备的开发、测试和使用，特制定本标准。

基于SIM卡的数字身份 身份鉴别设备技术要求

1 范围

本文件规定了基于SIM卡的数字身份身份鉴别设备的系统组成、技术要求和安全要求等。

本文件适用于基于SIM卡的数字身份身份鉴别设备，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 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

3 术语和定义

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

3.1

身份鉴别设备 Identity authentication device

须集成身份鉴别设备专用安全芯片的NFC终端，用于受理身份鉴别凭证读取、验证等业务。

[来源：T/OIDAA XXXX-XXXX 基于SIM卡的数字身份 技术框架，4.8]

4 概述

身份鉴别设备总体技术架构如图1所示，身份鉴别设备功能模块包括采集模块、外部接口、MCU、安全芯片、通讯模块等，通过通讯模块与外部接口，实现与业务前端对接及身份鉴别应用服务端交互。

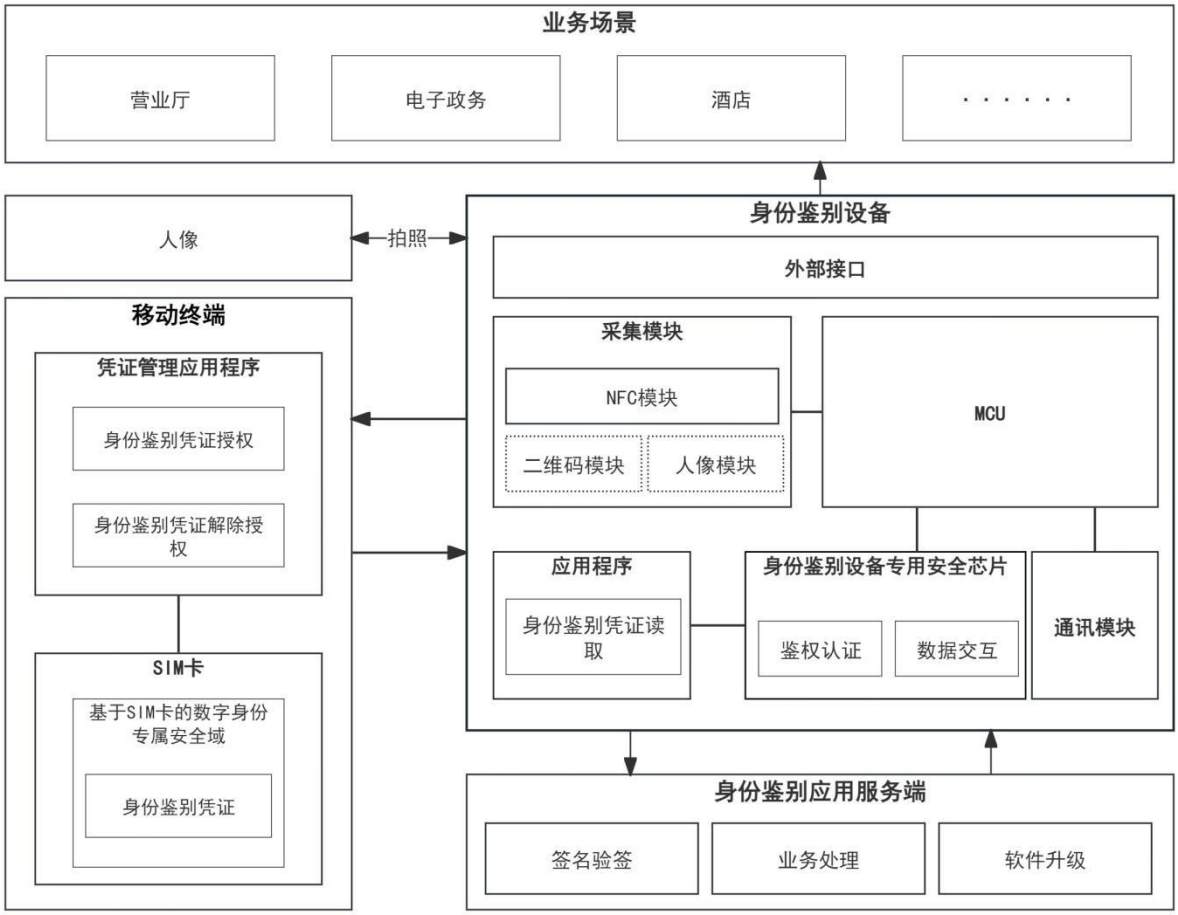

图 1 身份鉴别设备通用技术架构

采集模块：定义身份鉴别设备业务处理所需的模块，如NFC模块、人像模块、二维码模块等。

外部接口：定义身份鉴别设备对接业务前端接口，如USB接口。

MCU：定义身份鉴别设备用于控制和执行各种任务，如人像采集、NFC模块通信、数据处理、通信、控制和调度等。

身份鉴别设备专用安全芯片：身份鉴别设备专用的含有密码算法、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。身份鉴别设备通过身份鉴别设备专用安全芯片可实现读取SIM卡中的身份鉴别凭证等数据、可与卡应用进行身份认证等功能。

通讯模块：定义身份鉴别设备存储数据联网通信能力的专用模块。

身份鉴别设备与身份鉴别应用服务端之间的安全通信要求不属于本规范约束范围。

5 技术要求

5.1 硬件要求

5.1.1 NFC 读卡模块

a) 支持 ISO/IEC 14443 TypeA/B 协议；
b) 支持以 13.56MHz 射频载波通信；
c) 可支持 TypeA/B 协议自动切换。

5.1.2 二维码模块

可选支持
a) 可支持 30W 及以上像素；
b) 可支持扫描二维码功能(分辨率：640×480 以上 CMOS 码制：二维码支持补光)。

5.1.3 人像模块

可选支持
a) 支持人像采集；
b) 支持双目 200W 及以上像素；
c) 支持人像活体检测。

5.1.4 其他

a) 宜支持语音提示；
b) 宜支持图文提示。

5.2 外部接口

支持有线或无线通信接口。

5.3 MCU

5.3.1 硬件要求

a) 主频 600MHz 及以上；
b) 内存 2M bytes 及以上；
c) 可支持 SM2、SM3、SM4 算法。

5.3.2 数据运营

a) 可支持用户核验信息实时上报；
b) 可支持设备运行信息监控、上报。

5.4 通讯模块

5.4.1 基本能力

a) 支持应用动态下载能力；
b) 支持应用远程管理能力。

5.4.2 网络连接

可支持多种网络连接方式包括：
a) 支持 4G 及以上模块；
b) 支持 WIFI 模块；
c) 支持协议：TCP/IP、HTTP 等常用协议。

5.5 其他要求

5.5.1 工作环境

设备应在下述环境下正常工作，且不致引起外观和机械结构以及基本功能受损:

a) 环境温度：0℃～45℃；
b) 相对湿度：20%～90%。

6 安全要求

6.1 设备安全要求

6.1.1 硬件接口安全要求

硬件接口应符合以下安全要求：

a) 对于使用无线和有线外围接口的设备,宜通过指示灯或显示屏等方式,提供连接状态的监控功能;
b) 对于具有调试功能的接口,应在出厂时设置为默认关闭。

6.1.2 设备标识安全

身份鉴别设备的标识应符合以下安全要求：

a) 硬件整机应具备唯一的识别码作为设备的唯一性身份标识；
b) 设备的唯一标识应具备防篡改机制；
c) 对于预装有软件及可以进行软件升级的设备，应对预装软件、补丁包/升级包的不同版本进行唯一性标识，版本唯一性标识方式包括但不限于版本号。

6.1.3 访问控制安全要求

身份鉴别设备的访问控制功能应符合以下安全要求：

a) 默认状态下应仅开启必要的服务和对应的端口；
b) 在用户访问受控资源时，支持设置访问控制策略并依据设置的控制策略进行授权和访问控制，确保访问和操作安全。

6.1.4 专用芯片安全要求

专用芯片安全应符合《T/OIDAA XXX 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》相关要求。

6.2 信息安全要求

6.2.1 控制信息安全要求

设备控制应符合以下安全要求：

a) 设备可支持用户核验信息实时上报；
b) 可支持设备运行信息监控、上报。

6.2.2 个人信息安全要求

个人信息在采集、传输、存储、使用过程中，应满足以下要求：

a） 对个人信息的采集应按照 GB/T 35273 第 5 章中个人信息的采集规定执行，若涉及人像采集应按照 GB/T 35678—2017 中的图像技术要求执行。
b） 应采用密码算法保证个人信息在设备采集、传输、存储、使用的安全性和不可篡改性；
c） 针对生物特征识别信息的保护要求，还应符合 GB/T40660-2021 的规定；
d） 应采用密码技术保证远场和近场通信过程中个人信息的保密性、完整性、不可否认性、真实性；
e） 在实现身份鉴别功能后，应按照敏感个人信息处理规则，及时对敏感个人信息进行处理。

参 考 文 献

[1] GA/T 1721—2020 居民身份网络认证 通用术语