

团体标准

T/OIDAA XXX—XXXX

基于 SIM 卡的数字身份 移动终端技术要求

Digital Identity Based On SIM Card

Technical Requirements For Mobile Terminals

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

目次 1

前言 2

引言 3

1 范围 4

2 规范性引用文件 4

3 术语和定义 4

4 技术要求 4

参考文献 6

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、兴唐通信科技有限公司、楚天龙股份有限公司、北京握奇数据股份有限公司、天翼电子商务有限公司、前海联大（深圳）技术有限公司、厦门中盾安信科技有限公司、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、林晓飞、刘金地、王性国、果艳红、蔡子凡、朱志高、赵轶、梁栋、陈乐、林福鹏、周鹏。

本标准版权归中关村安信网络身份认证产业联盟所有。未经事先书面许可，本标准的任何部分不得以任何形式或任何手段进行复制、发行、改编、翻译、汇编或将本标准用于其他任何商业目的。

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。

为统一规范移动终端提供身份鉴别凭证认证的能力,指导移动终端的开发、测试和使用,并定义移动终端的通信要求、系统要求、核验要求等,特制定本部分。

基于 SIM 卡的数字身份 移动终端技术要求

1 范围

本文档的主要内容是“基于SIM卡的数字身份”系列规范中移动终端的技术要求，规定支撑基于SIM卡的身份鉴别服务，移动终端的通用、安全等技术参数要求。

本文档是适用于基于SIM卡的数字身份和研发移动终端产品的生态应用，并适用于相关系统的设计、开发、测试和应用。

本文档规定了“基于SIM卡的数字身份”的技术要求，为使用基于SIM卡的数字身份和研发移动终端产品提供技术依据。

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，凡是注日期的引用文件，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 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 35276—2017 信息安全技术 SM2密码算法使用规范
GB/T 37729—2019 信息技术 智能移动终端应用软件（APP）技术要求
GPD_Open Mobile API Specification 3.3—2018 信息安全技术 OMA接口规范
GPD_SE_Access_Control 1.1—2014 信息安全技术 安全单元接入控制规范
GPC_CardSpecification_v2.3.1—2018 信息安全技术 GP智能卡规范

3 术语和定义

T/OIDAA XXX—XXXX界定的以及下列术语和定义适用于本文件。

3.1 术语、定义和缩略语

BIP 独立承载协议 (Bearer Independent Protocol)

4 技术要求

移动终端应是一种具备网络连接能力，具备屏幕彩色显示，能够安装智能应用或小程序，能为用户扩展打造安全使用基于SIM卡的数字身份的设备。并且可以根据应用场景和SIM卡不同功能模块实现不同等级的安全产品。

4.1 通信要求

4.1.1 蜂窝网络要求

移动终端需要支持中国运营商蜂窝网络，支持 BIP 相关主动式命令，支持数据短信功能。

4.1.2 接触式智能卡支持要求

移动终端需要遵循支持智能卡接触相关规范，支持 ISO/IEC 7816 协议。

4.1.3 NFC 要求

移动终端需要支持 NFC 功能，支持读写器模式，支持卡模拟模式，支持点对点模式。

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

4.2 系统要求

4.2.1 USAT 功能要求

移动终端的系统需要支持 STK 和 USAT 相关功能。具体可参考 ETSI TS 102 223、3GPP TS 31.111 等系列相关规范。

4.2.2 卡槽支持要求

多卡槽的设备，至少支持卡槽 1 和应用软件的安全通信。

4.2.3 数据交互要求

终端系统需要能够和 SIM 卡建立安全的数据通道，解析卡内访问规则，可参考 OMA、GP 等相关标准规范。

4.3 核验要求

4.3.1 PIN 核验要求

支持 4-8 位 PIN 校验。

4.3.2 生物核验要求

支持人脸或者指纹等安全校验。

参 考 文 献
