ICS 67.140.10
CCS X 55

团　　体　　标　　准

T/OIDAA XXX—XXXX

基于SIM卡的数字身份 技术框架

Digital identity based on SIM card—technical framework

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：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、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、厦门中盾安信科技有限公、前海联大（深圳）技术有限公司、芯昇科技有限公司、北京握奇数据股份有限公司、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、熵基科技股份有限公司、全民认证科技（杭州）有限公司、四川科道芯国智能技术股份有限公司、上海复旦微电子集团股份有限公司、北京中广瑞波科技股份有限公司、楚天龙股份有限公司、恒宝股份有限公司、鼎特(北京)信息技术有限公司、天地融科技股份有限公司、海十联（上海）智能科技有限公司、北京仁叁文化有限公司。

起草人：管毅、黄炜耀、张新彬、曹卫然、果艳红、王性国、梁斌、张林、梁栋、蔡子凡、许雪姣、王剑冰、林尧禹、范博贺、李中敏、李旦、高云鹏、吴朕阳、霍红文、杜平、段延方、周鹏、李伯茹、吕征、王迪、周建、范嵬。

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。

为更好实现权威数字身份和SIM卡融合，建立统一、安全、便捷的身份鉴别技术框架，构建身份鉴别服务生态环境，特制定本标准。

基于SIM卡的数字身份 技术框架

1 范围

本文件给出了基于SIM卡的数字身份技术框架，规定了基于SIM卡的数字身份的系统组成、业务功能和技术要求。

本文件适用于基于SIM卡的数字身份的设计、开发、集成、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 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

T/OIDAA xx-xxxx 基于SIM卡的数字身份 身份鉴别设备技术要求

3 缩略语

下列缩略语适用于本文件。

BIP 独立承载协议（Bearer Independent Protocol）

NFC 短距离无线通信技术（Near Field Communication）

SIM 用户身份模块（Subscriber Identity Module）

SMS 短信（Short Message Service）

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

SM3 SM3密码杂凑算法（SM3 cryptographic hash algorithm）

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

TSM 可信服务管理（Trusted Service Manager）

USAT USIM应用工具包（USIM Application Toolkit）

4 术语和定义

4.1

身份鉴别 identity authentication

验证用户所声称身份的过程。

[来源：GB/T 42573—2023，3.5]

4.2

身份鉴别凭证 Identity verification certificate

用于在网络空间中证明居民个人身份信息的电子文件，与居民身份证件具有一一对应关系。

4.3

移动终端 Mobile terminal

装载SIM卡及实现身份鉴别凭证授权与身份鉴别凭证解除授权等能力的软硬件组合。

4.4

电信运营商TSM平台 Telecom operator TSM platform

与SIM卡、居民身份网络认证服务系统交互，受理安全域创建、安全域删除、安全域锁定、安全域解锁等请求，并下发到SIM卡应用中的软硬件组合。

4.5

基于SIM卡的数字身份 Digital identity based on SIM card

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，需通过身份鉴别设备访问，以实现自然人的身份鉴别服务。

4.6

基于SIM卡的数字身份专属辅助安全域 Supplementary Security Domain for digital identity based on SIM card

一个专门分配给基于SIM卡的数字身份使用的受保护的区域，用于存储敏感数据和执行安全相关操作。

4.7

居民身份网络认证服务系统 Cyber Trusted identity online authentication service system

接收身份鉴别凭证管理应用程序和身份鉴别应用服务端的请求，返回处理结果，并集中安全存储身份鉴别凭证和居民身份网络标识的服务系统。

4.8

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。

4.9

身份鉴别应用服务端 Identity authentication application server

与身份鉴别设备、居民身份网络认证服务系统交互，接收身份鉴别等业务请求并提交到居民身份网络认证服务系统的软硬件组合。

4.10

安全芯片 Security chip

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。

4.11

数字身份卡应用 Digital identity card applet

一种运行在SIM卡数字身份专属辅助安全域中的应用程序。

5 总则

5.1 系统框架

基于SIM卡的数字身份技术框架由居民身份网络认证服务系统、移动终端、身份鉴别设备、身份鉴别应用服务端和电信运营商TSM平台五个部分组成。

图1 基于SIM卡的数字身份技术框架

在基于 SIM 卡的数字身份技术框架中，身份鉴别凭证贯穿于可信身份认证的所有业务流程中：

a）身份鉴别凭证授权：居民通过移动终端的凭证管理应用程序向居民身份网络认证服务系统申请下载身份鉴别凭证，并把身份鉴别凭证写入SIM卡；

b）身份鉴别凭证解除授权：居民通过移动终端的凭证管理应用程序向居民身份网络认证服务系统申请解除授权身份鉴别凭证，并删除SIM卡中的身份鉴别凭证；

c）身份鉴别凭证读取：身份鉴别设备读取居民SIM卡中的身份鉴别凭证；

d）身份鉴别凭证验证：身份鉴别设备将读取的身份鉴别凭证通过身份鉴别应用服务端和居民身份网络认证服务系统协同交互实现身份鉴别凭证验证。

6 业务功能

6.1 移动终端

6.1.1 凭证管理应用程序

6.1.1.1 身份鉴别凭证授权

居民通过凭证管理应用程序的身份鉴别凭证授权功能，在居民身份网络认证服务系统申请下载身份鉴别凭证并把身份鉴别凭证写入SIM卡。授权身份鉴别凭证时，凭证管理应用程序需采集居民身份证件信息和人脸图像，提交到居民身份网络认证服务系统。

6.1.1.2 身份鉴别凭证解除授权

居民通过凭证管理应用程序的身份鉴别凭证解除授权功能，在居民身份网络认证服务系统申请解除授权身份鉴别凭证，并删除SIM卡中的身份鉴别凭证，删除后此身份鉴别凭证直接失效。解除授权身份鉴别凭证时，凭证管理应用程序需读取居民身份证件信息或读取身份鉴别凭证信息并采集人脸图像，提交到居民身份网络认证服务系统。

6.1.2 SIM 卡

6.1.2.1 基于 SIM 卡的数字身份专属安全域

基于SIM卡的数字身份专属安全域是在SIM卡上创建的专属辅助安全域，为基于SIM卡的数字身份提供数据安全存储空间。

6.2 居民身份网络认证服务系统

6.2.1 身份鉴别凭证管理服务接口

身份鉴别凭证管理服务接口主要与移动终端进行数据交互，实现协议的解析、签名验签以及业务服务的分发和调度等功能。

6.2.2 身份鉴别服务接口

身份鉴别服务接口主要与身份认证应用服务端进行数据交互，实现协议的解析、签名验签以及业务服务的分发和调度等功能。

6.2.3 签名验签

提供签名和验签服务，验证数据的完整性和有效性；服务使用算法应符合 GB/T 0009—2023《SM2密码算法使用规范》的要求。

6.2.4 业务服务

6.2.4.1 身份鉴别凭证管理

根据身份鉴别凭证管理服务接口接收的功能请求，实现身份鉴别凭证的授权和解除授权等功能。

6.2.4.2 身份鉴别凭证验证

根据身份鉴别服务接口接收的功能请求，实现身份鉴别凭证验证等功能。

6.2.4.3 标识管理

实现居民身份网络标识的存储、查询、更新和删除等功能。

6.2.4.4 SIM卡空间管理

与电信运营商TSM平台进行交互，实现协议的解析、安全域创建、安全域删除、安全域锁定和安全域解锁、应用个人化等功能。

6.2.5 数据存储

实现身份鉴别凭证和居民身份网络标识等业务数据存储功能。

6.3 身份鉴别设备

6.3.1 数据读取与身份鉴别凭证验证

身份鉴别设备通过专用安全芯片读取SIM卡中身份鉴别凭证，并将读取的身份鉴别凭证通过身份鉴别应用服务端和居民身份网络认证服务系统协同交互实现身份鉴别凭证验证。

6.4 身份鉴别设备专用安全芯片

6.4.1 鉴权认证

身份鉴别设备通过身份鉴别设备专用安全芯片与卡应用进行身份认证；认证使用算法应符合GB/T 35276—2017《信息安全技术 SM2密码算法使用规范》、GB/T 32907—2016《信息安全技术 SM4分组密码算法》的要求。

6.4.2 数据交互

身份鉴别设备通过身份鉴别设备专用安全芯片读取SIM卡中的身份鉴别凭证等数据。数据读取使用算法应符合GB/T 35276—2017《信息安全技术 SM2密码算法使用规范》、GB/T 32907—2016《信息安全技术 SM4分组密码算法》的要求。

6.5 身份鉴别应用服务端

身份鉴别应用服务端是身份鉴别设备的后台服务，主要功能是对身份鉴别设备发送的数据包按照居民身份网络认证服务系统的身份鉴别服务接口要求进行组包和签名，居民身份网络认证服务系统对数据包进行验签、解析和身份鉴别凭证验证，并把结果转发至身份鉴别设备。

6.5.1 签名验签

提供签名和验签服务，验证数据的完整性和有效性；服务使用算法应符合 GB/T 0009—2023《SM2密码算法使用规范》的要求。

6.6 电信运营商 TSM 平台

实现基于SIM卡的数字身份专属安全域的创建、删除、锁定、解锁等能力。

7 技术要求

7.1 一般要求

基于SIM卡的数字身份系统业务功能的具体技术要求应符合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》、T/OIDAA xx-xxxx《基于SIM卡的数字身份 身份鉴别设备技术要求》。

7.2 居民身份网络认证服务系统

7.2.1 身份鉴别凭证管理服务接口

身份鉴别凭证管理服务接口技术要求如下：

a) 应实现协议的解析；
b) 应调用签名验签服务对交互数据进行签名和验签，实现对请求的合法性验证；
c) 应进行业务服务分发和调度。

7.2.2 身份鉴别服务接口

身份鉴别凭证应用服务接口技术要求如下：

a) 应实现协议的解析；
b) 应调用签名验签服务对交互数据进行签名和验签，实现对请求的合法性验证；
c) 应进行业务服务分发和调度；
d) 应符合 T/OIDAA XXXX《基于 SIM 卡的数字身份 身份鉴别服务接口要求》的要求。

7.2.3 业务服务

业务服务技术要求如下：

a) 应提供身份鉴别凭证管理、标识管理、身份鉴别凭证验证、SIM 卡空间管理等功能；
b) 应符合 T/OIDAA xx-xxxx《基于 SIM 卡的数字身份 NFC 身份鉴别流程》的要求。

7.2.4 数据存储

数据存储技术要求如下：

a) 应实现身份鉴别凭证和居民身份网络标识等数据安全存储功能；
b) 数据存储应有灾备机制。

7.3 移动终端

移动终端技术要求如下：

a) 应支持电信运营商蜂窝网络、接触式智能卡和 NFC 功能；

b) 应支持 USAT 功能；

c) 应符合 T/OIDAA xx-xxxx《基于 SIM 卡的数字身份 移动终端技术要求》的要求。

7.3.1 SIM 卡

SIM 卡技术要求如下：

a) 应实现身份鉴别凭证存储和读取等功能；

b) 应符合 T/OIDAA xx-xxxx《基于 SIM 卡的数字身份 SIM 卡技术要求》；

c) 应符合 T/OIDAA xx-xxxx《基于 SIM 卡的数字身份 SIM 卡接口要求》的要求。

7.3.2 凭证管理应用程序

应实现身份鉴别凭证授权和身份鉴别凭证解除授权等功能。

7.4 身份鉴别设备

应实现身份鉴别凭证认证、数据读取等功能。

7.4.1 身份鉴别设备专用安全芯片

身份鉴别设备专用安全芯片技术要求如下：

a) 应实现身份鉴别设备通过集成该芯片与卡应用进行外部认证、读取 SIM 卡中的数字身份数据；

b) 应符合 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》的要求；

c) 应符合 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》的要求。

7.5 身份鉴别应用服务端

应实现签名验签、业务处理等功能。

7.6 电信运营商 TSM 平台

电信运营商TSM平台技术要求如下：

a）应实现卡空间管理能力；

b）应具备通过BIP、短信等通道访问SIM卡能力。

参 考 文 献

[1] GB/T 32907-2016 信息安全技术SM4分组密码算法
[2] GB/T 32918.1-2016 信息安全技术SM2椭圆曲线公钥密码算法第1部分：总则
[3] GB/T 32918.2-2016 信息安全技术SM2椭圆曲线公钥密码算法第2部分：数字签名算法
[4] GB/T 32918.3-2016 信息安全技术SM2椭圆曲线公钥密码算法第3部分：密钥交换协议
[5] GB/T 32918.4-2016 信息安全技术SM2椭圆曲线公钥密码算法第4部分：公钥加密算法
[6] GB/T 32918.5-2017 信息安全技术SM2椭圆曲线公钥密码算法第5部分：参数定义
[7] GB/T 33560-2017 信息安全技术密码应用标识规范
[8] GB/T 35275-2017 信息安全技术SM2密码算法加密签名消息语法规范
[9] GB/T 0009—2023 SM2密码算法使用规范
[10] GM/T 0008-2012 安全芯片密码检测准则
[11] 《“互联网+”可信身份认证平台应用实施指南（试行）》(公科信〔2017〕209号，2017年11月7日发布)