ICS 67.140.10
CCS X 55

团　　体　　标　　准

T/OIDAA XXX—XXXX

基于SIM卡的数字身份　身份鉴别服务接口要求

Digital identity based on SIM card—

Authentication service interface requirements

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

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司

芯昇科技有限公司、北京仁叁文化有限公司、北京握奇数据股份有限公司。

起草人：张新彬、高诚、林晓飞、刘艳春、果艳红、王性国、梁斌、张林、梁栋、蔡子凡、许雪姣、叶建宝、徐璐、范嵬、赵轶。

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。

为统一规范提供身份鉴别凭证验证服务的能力，指导身份鉴别应用服务端进行软件开发、对接和使用，并定义身份鉴别应用服务端和身份鉴别凭证服务之间的交互流程、通信协议以及传输的数据格式等，特制定本部分。

基于SIM卡的数字身份　身份鉴别服务接口要求

1　范围

T/OIDAA XXX—XXXX 的本部分规定了居民身份网络认证服务系统中身份鉴别服务接口（以下简称“服务接口”）的作用、功能、使用要求和接口定义描述。

本部分适用于居民身份网络认证服务系统的服务接口的设计和开发。

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。

T/OIDAA XXXXX 基于SIM卡的数字身份　技术框架

GB/T 35678-2017　公共安全人脸识别应用　图像技术要求

3　缩略语

下列缩略语适用于本文件。

API　应用编程接口（Application Programming Interface）

HTTPS　文本传输安全协议（Hypertext Transfer Protocol Secure）

JSON　JavaScript标记（JavaScript Object Notation）

URL　统一资源定位符（Uniform Resource Locator）

4　术语和定义

T/OIDAA XXXXX 《基于SIM卡的数字身份　技术框架》界定的术语和定义适用于本文件。

5　接口概述

服务接口包括接口功能、交互方式和使用要求。

5.1　接口功能

服务接口主要提供基于NFC的身份鉴别服务。

5.2　接口交互方式

接口交互中服务端（居民身份网络认证服务系统）与客户端（身份鉴别终端）之间采用HTTPS协议进行传输，数据交换格式为JSON，服务通过POST方式访问URL：

https://[host]:[port]/did/main/bs/[interface]。

其中：

[host]：服务IP或者域名；
[port]：服务端口号；
[interface]：服务接口名称。

5.3 接口使用要求

身份鉴别凭证验证服务通过“身份鉴别授权”和“身份鉴别凭证验证”两次交互完成：
a）身份鉴别应用服务端向居民身份网络认证服务系统发起身份鉴别授权请求并获取响应；
b）身份鉴别应用服务端向居民身份网络认证服务系统发起身份鉴别凭证验证请求并获取响应。
服务流程见图 1。

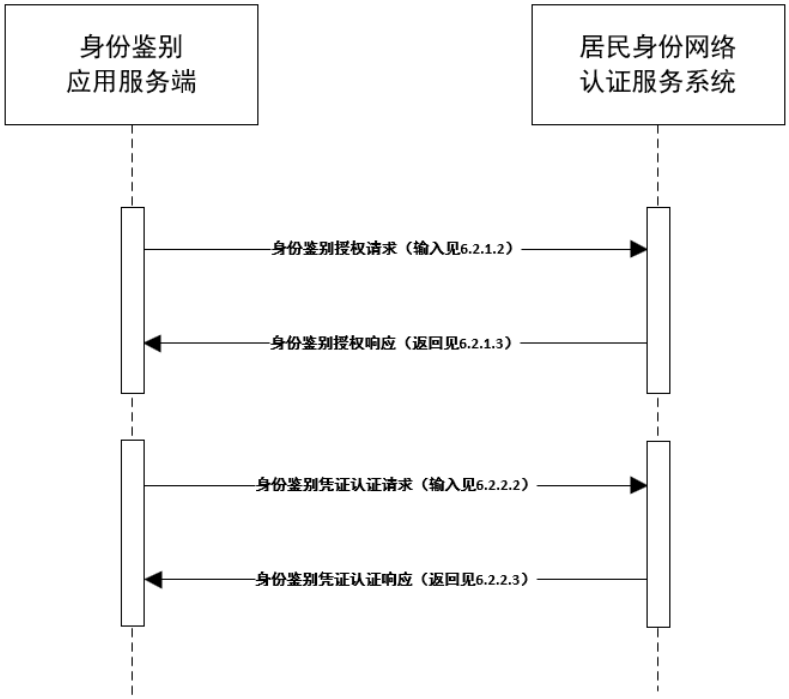

图 1 身份鉴别凭证验证服务流程

6 接口定义

6.1 概述

服务接口的数据传输内容见表1，采用JSON格式数据传输格式并使用HTTPS协议通信。

表 1 数据传输格式说明

数据项	标识符	约束条件	说明
请求头	gp_bsn	可选	业务流水号
	gp_orgID	必选	机构ID
	gp_appID	必选	应用ID
	gp_salt	必选	时间戳（秒）|随机数

	gp_sign_version	必选	签名密钥版本号
	gp_enc_version	必选	加密密钥版本号
	gp_sign	必选	签名值，请求头和请求业务数据集签名结果的 Base64 编码字符串
请求体	reqBody	必选	请求业务数据集，JSON 格式，6.2 中的输入参数基于此项进行说明
响应头	gp_sign	必选	签名值,响应业务数据集签名结果的 Base64 编码字符串。
响应体	respBody	必选	响应业务数据集，JSON 格式，6.2 中的返回值基于此项进行说明

6.2 身份鉴别凭证验证服务

6.2.1 身份鉴别授权

6.2.1.1 接口名称

身份鉴别授权URL中[interface]=universal-grant。

6.2.1.2 输入参数

身份鉴别授权输入参数格式见表2。

表 2 身份鉴别授权输入参数说明

数据项	标识符	约束条件	说明
业务类型	bizType	必选	业务类型,取值如下： “4”-表示身份鉴别设备线下读取
芯片序列号	chipSn	必选	身份鉴别设备专用安全芯片序列号

6.2.1.3 返回值

身份鉴别授权返回值格式见表 3、表 4。

表 3 身份鉴别授权返回值说明

数据项	标识符	约束条件	说明
业务流水号	bsn	必选	业务流水号
响应码	resultCode	必选	业务处理返回码
响应描述	resultDesc	必选	响应信息描述
响应数据	data	必选	业务成功时，值不为空

表 4 身份鉴别凭证验证返回值-data 说明

数据项	标识符	约束条件	说明
授权令牌	grantToken	可选	身份鉴别凭证验证业务授权令牌

6.2.2 身份鉴别凭证验证

6.2.2.1 接口名称

身份鉴别凭证验证URL中[interface]=netcert-auth。

6.2.2.2 输入参数

身份鉴别凭证验证输入参数格式见表 5。

表 5 身份鉴别凭证验证输入参数说明

数据项	标识符	约束条件	说明
应用名称	appName	必选	用于接入居民身份网络认证服务系统的应用程序名称，长度小于等于32
业务序列号	bizSeq	必选	由调用方生成，仅限字母数字，长度32位，要求唯一
身份鉴别凭证数据	netcertData	必选	身份认证应用终端读取返回的身份鉴别凭证数据
人像加密数据	photoEncData	必选	使用分配给机构的密钥加密数据，加密方式为数字信封，以 base64 编码输出，详见附录 A。人像原始数据要求如下： 1)长度大于等于 10K，小于等于 70K。 2) 人脸图像符合《GB/T 35678- 2017 公共安全人脸识别应用中 人脸图像技术要求》 3）人脸图像格式支持JPEG、PNG、BMP

6.2.2.3 返回值

身份鉴别凭证验证返回值格式见表 6、表 7。

表 6 身份鉴别凭证验证返回值说明

数据项	标识符	约束条件	说明
业务流水号	bsn	必选	业务流水号
响应码	resultCode	必选	业务处理返回码
响应描述	resultDesc	必选	响应信息描述
响应数据	data	必选	业务成功时，值不为空

表 7 身份鉴别凭证验证返回值-data 说明

数据项	标识符	约束条件	说明
身份标识	BID	可选	
人脸比对分数	photoCompareScore	可选	人脸比对相似度判定 阈值为 700 分； 700 分对应 0.01%认假率， 800 分对应 0.001%认假率， 900 分对应 0.0001%认假率。

附 录 A
（资料性附录）
数字信封格式说明

A.1 数据信封格式

A.1.1 概述

数字信封由SM2密文和SM4密文组成，其中SM2算法标识为：1.2.156.10197.1.301.3，排序方式为C1C3C2，用于加密SM4密钥；SM4算法标识为：1.2.156.10197.1.104，分组方式为：ECB，填充方式为：PKCS5，用于加密业务数据,SM4 加密密钥在每次计算过程中动态生成。最终密文经 ASN.1-DER-TLV 编码后，以Base64形式输出，数据结构参考下图2。

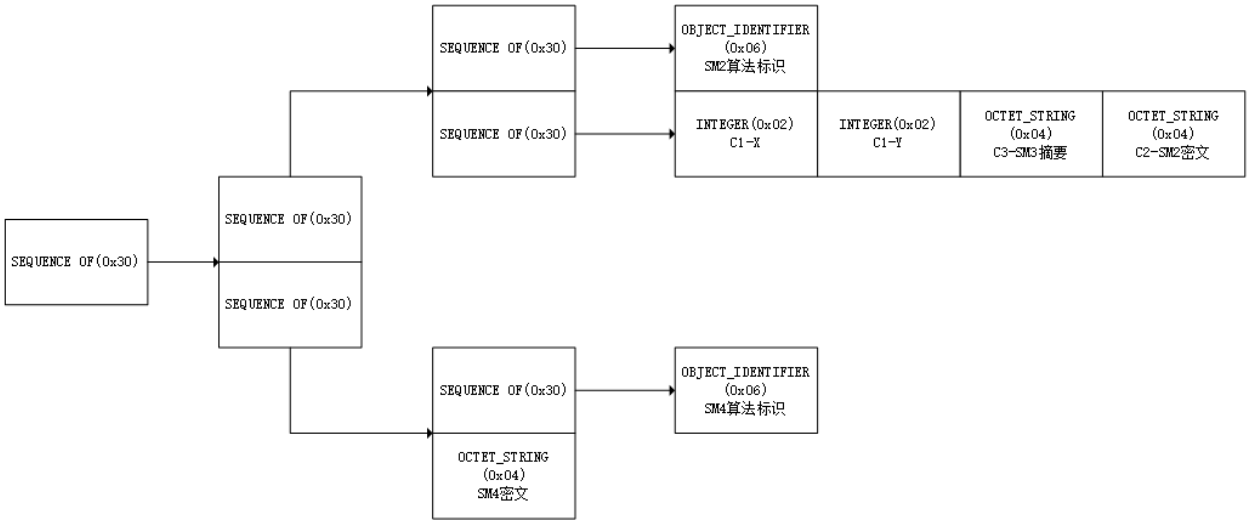

图2 数字信封数据结构

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 0009—2023 SM2密码算法使用规范
[3] ECMA-404 The JSON Data Interchange Standard
[4] RFC 3548 The Base16, Base32, and Base64 Data Encodings