



# 中华人民共和国公共安全行业标准

GA/T XXXX.2—XXXX

## 居民身份网络认证 认证服务 第2部分： 服务接口要求

CTID online authentication—Authentication services—Part 2: Requirements for  
service interface

(报批稿)

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中华人民共和国公安部 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、定义和缩略语 .....	1
3.1 术语和定义 .....	1
3.2 缩略语 .....	1
4 总则 .....	1
4.1 概述 .....	1
4.2 作用 .....	2
5 接口框架 .....	2
5.1 概述 .....	2
5.2 总体框架 .....	2
6 接口定义 .....	4
6.1 概述 .....	4
6.2 身份认证服务 .....	4
6.3 网证下载服务 .....	6
6.4 认证结果 .....	8
参考文献 .....	9
图 1 居民身份网络认证系统整体技术框架 .....	2
图 2 身份认证服务流程 .....	3
图 3 网证下载服务流程 .....	4
表 1 数据传输格式说明 .....	4
表 2 身份认证申请输入参数说明 .....	5
表 3 身份认证申请返回值说明 .....	5
表 4 身份认证输入参数说明 .....	6
表 5 身份认证返回值说明 .....	6
表 6 网证下载申请输入参数说明 .....	7
表 7 网证下载申请返回值说明 .....	7
表 8 网证下载输入参数说明 .....	8
表 9 网证下载返回值说明 .....	8
表 10 认证结果说明 .....	8

## 前 言

GA/T XXXX《居民身份网络认证 认证服务》分为五个部分：

- 第1部分：认证分级；
- 第2部分：服务接口要求；
- 第3部分：信息获取控件接口要求；
- 第4部分：人脸图像采集控件技术要求；
- 第5部分：人脸比对引擎接口要求。

本部分为GA/T XXXX的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文的发布机构不承担识别这些专利的责任。

本部分由公安部社会公共安全应用基础标准化技术委员会提出并归口。

本部分起草单位：公安部第一研究所、北京中盾安信科技发展有限公司、北京中盾安全技术开发公司、神思电子技术股份有限公司、浙江蚂蚁小微金融服务集团有限公司、北京数字认证股份有限公司、厦门身份宝网络科技有限公司、福建天创信息科技股份有限公司、广州大白互联网科技有限公司、公安部安全与警用电子产品质量检测中心。

本部分主要起草人：周卫东、王剑冰、吴国英、刘冰、谷晨、王昕、马文英、傅大鹏、黄佑君、蓝永文、续磊、张翔。

本部分为首次发布。

行业标准信息服务平台

## 引 言

居民身份网络认证是国家实施网络可信身份战略实施的重要环节之一。由于互联网的虚拟性特点,传统的身份认证方式已无法适应网络用户应用的需求,而网络身份认证存在着认证方式多种多样、身份信息真假难辨等弊端,并引发了数据泄露、身份冒用、隐私传播等新的安全问题,甚至威胁到了国家安全。为此,亟需从标准化角度开展研究,构建安全、便捷、统一的居民身份网络认证技术框架,为在网络空间标识居民身份和认证提供安全保障,为提高我国网络身份管理水平、实现网络社会治理现代化提供技术支持。

为统一规范提供身份认证服务的能力,指导网证应用系统进行软件开发、对接和使用,并定义网证应用系统和身份认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。

行业标准信息服务平台



# 居民身份网络认证 认证服务 第2部分：服务接口要求

## 1 范围

GA/T XXXX的本部分规定了居民身份网络认证服务系统中网证应用服务接口（以下简称“服务接口”）的作用、功能、使用要求和接口定义描述。

本部分适用于网证应用系统与居民身份网络认证服务系统之间的网证应用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。

- GA/T XXXX 居民身份网络认证 通用术语
- GA/T XXXX 居民身份网络认证 整体技术框架
- GA/T XXXX. 1 居民身份网络认证 认证服务 第1部分：认证分级
- GA/T XXXX. 3 居民身份网络认证 认证服务 第3部分：信息获取控件接口要求

## 3 术语、定义和缩略语

### 3.1 术语和定义

GA/T XXXX《居民身份网络认证 通用术语》界定的术语和定义适用于本文件。

### 3.2 缩略语

下列缩略语适用于本文件。

API：应用编程接口（Application Programming Interface）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

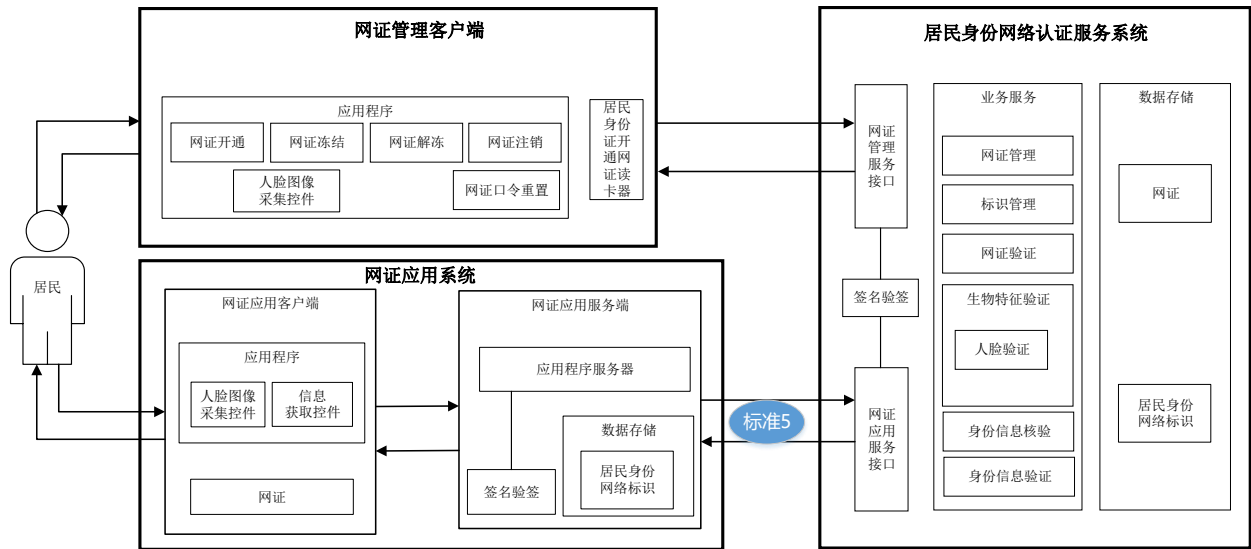
JSON：JavaScript标记（JavaScript Object Notation）

URL：统一资源定位符（Uniform Resource Locator）

## 4 总则

### 4.1 概述

在GA/T XXXX《居民身份网络认证 整体技术框架》给出的居民身份网络认证整体技术框架中，本部分规范的对象处于图1所示的“标准5”位置。



标准1.	居民身份网络认证	通用术语
标准2.	居民身份网络认证	整体技术框架
标准3.	居民身份网络认证	网络可信凭证和网络标识格式要求
标准4.	居民身份网络认证	认证服务 第1部分：认证分级
<b>标准5.</b>	<b>居民身份网络认证</b>	<b>认证服务 第2部分：服务接口要求</b>
标准6.	居民身份网络认证	认证服务 第3部分：信息获取控件接口要求
标准7.	居民身份网络认证	认证服务 第4部分：人脸图像采集控件技术要求
标准8.	居民身份网络认证	认证服务 第5部分：人脸比对引擎接口要求
标准9.	居民身份网络认证	信息采集设备 第1部分：居民身份证开通网证读卡器
标准10.	居民身份网络认证	信息采集设备 第2部分：自助开通网证设备
标准11.	居民身份网络认证	信息采集设备 第3部分：批量开通网证设备
标准12.	居民身份网络认证	信息采集设备 第4部分：移动终端安全技术要求

图1 居民身份网络认证系统整体技术框架

## 4.2 作用

居民身份网络认证服务系统的服务接口用于整体技术框架中网证应用系统与居民身份网络认证服务系统间的衔接，网证应用系统通过服务接口使用居民身份网络认证服务系统提供的服务。

## 5 接口框架

### 5.1 概述

接口框架包括总体框架和使用要求。

### 5.2 总体框架

#### 5.2.1 主要功能

服务接口主要提供身份认证和网证下载服务。

#### 5.2.2 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（网证应用服务端）之间采用HTTP协议进行传输，数据交换格式为JSON，服务通过POST方式访问URL：

http://[host]:[port]/ctid/api/[ver]/[interface]。

其中：

[host]：服务IP或者域名；

[port]：服务端口号；

[ver]：服务API版本；

[interface]：服务接口名称。

### 5.2.3 使用要求

#### 5.2.3.1 身份认证服务使用要求

身份认证服务应符合GA/T XXXX. 1中认证分级对应认证因子的要求，通过“身份认证申请”和“身份认证”两次交互完成：

- 网证应用服务端向居民身份网络认证服务系统发起身份认证申请请求并获取响应；
- 网证应用服务端向居民身份网络认证服务系统发起身份认证请求并获取响应。

服务流程见图2。

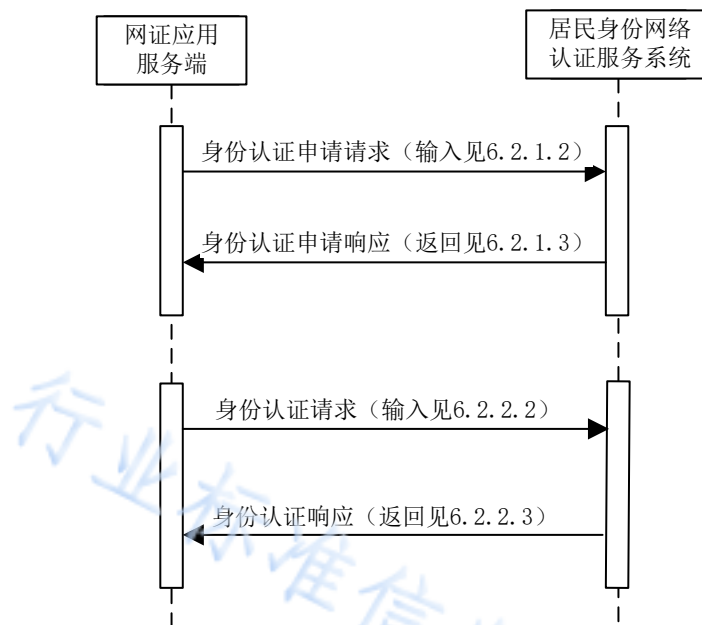


图2 身份认证服务流程

#### 5.2.3.2 网证下载服务使用要求

网证下载服务通过“网证下载申请”和“网证下载”两次交互完成：

- 网证应用服务端向居民身份网络认证服务系统发起网证下载申请请求并获取响应；
- 网证应用服务端向居民身份网络认证服务系统发起网证下载请求并获取响应。

服务流程见图3。

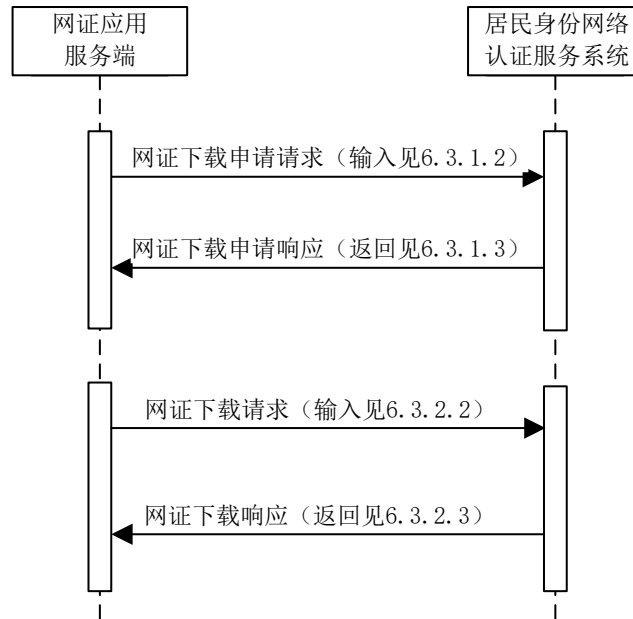


图3 网证下载服务流程

## 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HTTP协议通信。

表1 数据传输格式说明

数据项	标识符	表示格式	约束条件	说明
业务数据集	YWSJJ	o	必选	业务数据集，JSON 格式，6.2 中的输入参数和返回值均基于此项进行说明
签名值	QMZ	c1..900	必选	签名值，业务数据集签名结果的 Base64 编码字符串

### 6.2 身份认证服务

#### 6.2.1 身份认证申请

##### 6.2.1.1 接口名称

身份认证申请URL中[interface]=request。

##### 6.2.1.2 输入参数

身份认证申请输入参数格式见表2。

表2 身份认证申请输入参数说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
客户请求时间	KHQQSJ	c17	必选	格式为 YYYYDDMMhhmmss.sss
信息采集控件版本	XXCJKJBB	c19	可选	由 GA/T XXXX.3 5.3 中接口方法“获取控件版本号”获取
人脸图像采集控件版本	RLTXCJKJBB	c19	可选	人脸图像采集控件版本
保留数据	BLSJ	c19	可选	保留后续使用
认证分级代码	RZFJDM	c4	必选	认证分级代码取值如下： “0X63” - 对应 GA/T XXXX.1 的一级认证； “0X06” - 对应 GA/T XXXX.1 的二级认证； “0X16” - 对应 GA/T XXXX.1 的三级认证

### 6.2.1.3 返回值

身份认证申请返回值格式见表3。

表3 身份认证申请返回值说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
服务返回时间	FWFHSJ	c17	必选	格式为 YYYYDDMMhhmmss.sss
业务流水号	YWLSH	c1..32	必选	居民身份网络认证服务系统生成用来标识认证业务的编号
随机数	SJS	c120	必选	随机数的 Base64 编码
成功标志	CGBZ	c1..5	必选	成功标志：true/false。其中，true 代表服务访问成功，false 代表服务访问失败
错误信息描述	CWXXMS	c1..256	可选	错误信息描述

## 6.2.2 身份认证

### 6.2.2.1 接口名称

身份认证URL中[interface]=authentication。

### 6.2.2.2 输入参数

身份认证输入参数格式见表4。

表4 身份认证输入参数说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
客户请求时间	KHQQSJ	c17	必选	格式为 YYYYDDMMhmmss.sss
业务流水号	YWLSH	c1..32	必选	申请获取的业务流水号
认证分级	RZPJ	c4	必选	认证分级必须和认证申请中的一致
照片	ZP	c6827..54614	可选	照片数据的 Base64 编码
网证口令数据	WZKLSJ	c592..600	可选	由 GA/T XXXX.3 5.3 中接口方法“获取网证口令数据”获取
身份验证数据	SFYZSJ	c1..1304	可选	由 GA/T XXXX.3 5.3 中接口方法“获取身份验证数据”获取
认证保留数据	RZBLSJ	c1..54614	可选	认证保留数据的 Base64 编码

### 6.2.2.3 返回值

身份认证返回值格式见表5。

表5 身份认证返回值说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
服务返回时间	FWFHSJ	c17	必选	格式为 YYYYDDMMhmmss.sss
业务流水号	YWLSH	c1..32	必选	业务流水号
认证结果	RZJG	c4	必选	认证结果（见 6.4）
认证结果数据	RZJGSJ	o	可选	认证结果数据，为 JSON 格式
成功标志	CGBZ	c1..5	必选	成功标志：true/false。其中，true 代表服务访问成功，false 代表服务访问失败
错误信息描述	CWXXMS	c1..256	可选	错误信息描述

## 6.3 网证下载服务

### 6.3.1 网证下载申请

#### 6.3.1.1 接口名称

网证下载申请URL中[interface]=authDownloadRequest。

#### 6.3.1.2 输入参数

网证下载申请输入参数格式见表6。

表6 网证下载申请输入参数说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
客户请求时间	KHQQSJ	c1..17	必选	格式为 YYYYDDMMhhmmss.sss
信息采集控件版本	XXCJKJBB	c19	可选	由 GA/T XXXX.3 5.3 中接口方法“获取控件版本号”获取
人脸图像采集控件版本	RLTXCJKJBB	c19	可选	人脸图像采集控件版本
保留数据	BLSJ	c19	可选	保留数据
下载方式	XZFS	c4	必选	下载方式取值如下： “0X03” - 表示提交居民身份证件和网证口令进行下载； “0X02” - 表示提交居民身份证件和人脸数据进行下载

### 6.3.1.3 返回值

网证下载申请返回值数据格式见表7。

表7 网证下载申请返回值说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
服务返回时间	FWFHSJ	c1..17	必选	格式为 YYYYDDMMhhmmss.sss
业务流水号	YWLSH	c1..32	必选	业务流水号
随机数	SJS	c1..90	必选	随机数的 Base64 编码
成功标志	CGBZ	c1..5	必选	成功标志: true/false。其中, true 代表服务访问成功, false 代表服务访问失败
错误信息描述	CWXXMS	c1..256	可选	错误信息描述

### 6.3.2 网证下载

#### 6.3.2.1 接口名称

网证下载URL中[interface]=authenticationDownload。

#### 6.3.2.2 输入参数

网证下载输入参数格式见表8。

表8 网证下载输入参数说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
客户请求时间	KHQQSJ	c1..17	必选	格式为 YYYYDDMMhhmmss.sss
业务流水号	YWLSH	c1..32	必选	申请获取的业务流水号
下载方式	XZFS	c4	必选	下载方式必须和网证下载申请中的下载方式一致
照片	ZP	c6827..54614	可选	照片数据的 Base64 编码
网证口令数据	WZKLSJ	c592..600	可选	由 GA/T XXXX. 3 5. 3 中的接口方法“获取网证口令数据”获取
身份验证数据	SFYZSJ	c1..1304	可选	由 GA/T XXXX. 3 5. 3 中的接口方法“获取身份验证数据”获取
认证保留数据	RZBLSJ	c1..54614	可选	认证保留数据的 Base64 编码

### 6.3.2.3 返回值

网证下载返回值格式见表9。

表9 网证下载返回值说明

数据项	标识符	表示格式	约束条件	说明
业务站点编号	YWZDBH	c7	必选	由居民身份网络认证服务系统派发给网证应用系统的客户编号
客户应用名称	KHYPMC	c1..32	必选	网证应用系统应用的名称
服务返回时间	FWFHSJ	c17	必选	格式为 YYYYDDMMhhmmss.sss
业务流水号	YWLSH	c1..32	必选	业务流水号
网证数据	WZSJ	c1..250	可选	网证数据的 Base64 编码
成功标志	CGBZ	c1..5	必选	成功标志: true/false。其中: true 代表服务请求正常, false 代表服务请求异常
错误信息描述	CWXXMS	c1..256	可选	错误信息描述

### 6.4 认证结果

返回的认证结果为四位字符, 说明见表10。

表10 认证结果说明

认证结果字符	字符说明
第一字符	身份信息验证结果, 0: 通过, X: 未执行, 其他: 不通过
第二字符	人脸验证结果, 0: 通过, X: 未执行, 其他: 不通过
第三字符	网证验证结果, 0: 通过, X: 未执行, 其他: 不通过
第四字符	保留, 默认为X

### 参 考 文 献

- [1] GB/T 7408-2005 数据元和交换格式 信息交换 日期和时间表示法
  - [2] ECMA-404 The JSON Data Interchange Standard
  - [3] RFC 3548 The Base16, Base32, and Base64 Data Encodings
- 

行业标准信息服务平台