ICS 35.240.15
A 90

GA

# 中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

# 居民身份网络认证　整体技术框架

CTID online authentication—Overall technical framework

（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

本标准按照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。本文件的发布机构不承担识别这些专利的责任。

本标准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。

本标准起草单位：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、广东省公安厅、兴唐通信科技有限公司、浙江蚂蚁小微金融服务集团有限公司、联想（北京）有限公司、深圳市腾讯计算机系统有限公司。

本标准主要起草人：于锐、邱旭华、吴国英、张治安、黄耀晖、王菁、蔡子凡、谷晨、王昕、李俊、杨晓光、王俊峰、陈虎军、韩汨鸿。

本标准为首次发布。

# 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。

为了从国家层面构建网络身份管理体系，建立安全、便捷、统一的居民身份网络认证技术框架，从而推动建立不同网络服务提供者之间安全、合理、有序共享使用用户身份信息机制，构建网络可信身份服务生态环境，特制定本标准。

# 居民身份网络认证　整体技术框架

## 1　范围

本标准给出了居民身份网络认证整体技术框架,规定了居民身份网络认证系统的组成、业务功能和技术要求。

本标准适用于居民身份网络认证系统的设计、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 22239-2019 信息安全技术 网络安全等级保护基本要求

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　网络可信凭证和网络标识格式要求

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.2　居民身份网络认证　认证服务　第2部分：服务接口要求

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

GA/T XXXX.4　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

GA/T XXXX.5　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

GA/T XXXX.1　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

GA/T XXXX.2　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

GA/T XXXX.3　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

GA/T XXXX.4　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

GM/T 0054-2018　信息系统密码应用基本要求

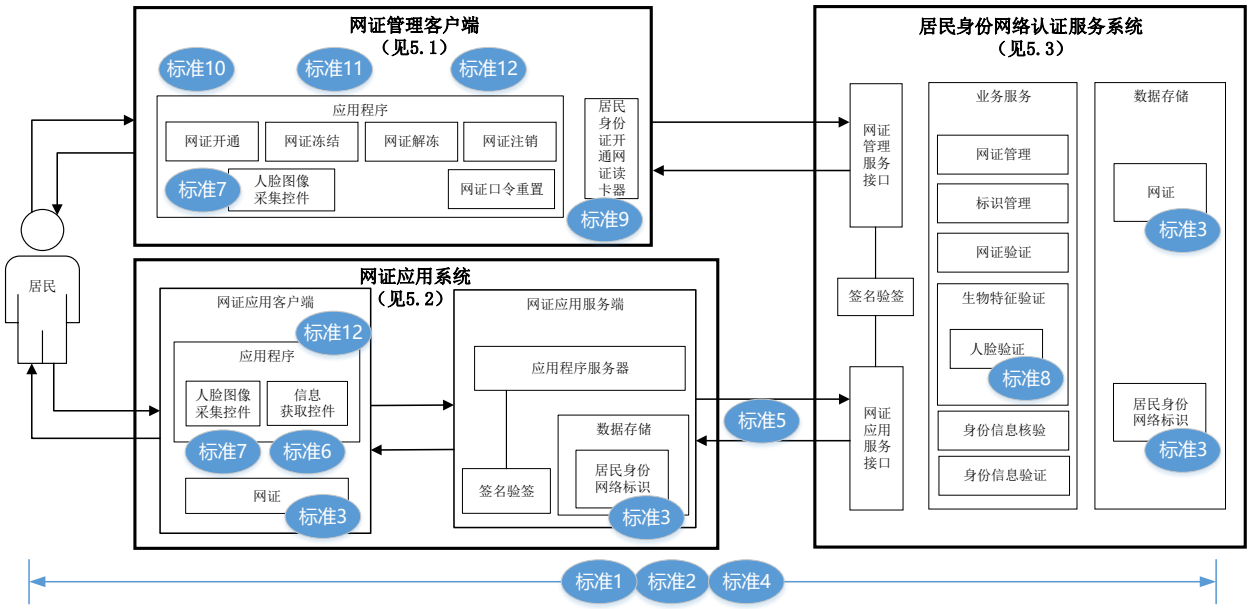
## 3　术语和定义

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。

## 4　总则

### 4.1　系统框架

居民身份网络认证系统由网证管理客户端、网证应用系统、居民身份网络认证服务系统三部分组成。居民身份网络认证系统整体技术框架见图1。




| | | | |
|---|---|---|---|
| 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 |
| 标准5 | 居民身份网络认证 | 认证服务 | 第2部分：服务接口要求 |
| 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**

在居民身份网络认证系统整体技术框架中，居民用网证证明身份，网证贯穿于居民身份网络认证的所有业务流程中：

a）网证开通申请：居民通过网证管理客户端与居民身份网络认证服务系统协同交互完成网证开通申请；

b）网证下载申请：居民开通网证后，通过网证应用系统与居民身份网络认证服务系统协同交互完成网证下载申请，把网证下载并存储到网证应用客户端；

c）身份认证：居民在网证应用系统中，办理需要核验身份的业务时，通过出示存储在网证应用客户端的网证，根据业务需求可同时附加人脸图像或网证口令等信息，由网证应用系统提交到居民身份网络认证服务系统核验居民身份的正确性；正确性核验通过后，居民身份网络认证服务系统向网证应用服务端下发验证结果和居民身份网络标识；

d）网证管理业务申请：居民通过网证管理客户端到居民身份网络认证服务系统进行网证注销、网证冻结、网证解冻和网证口令重置等操作，实现对网证的管理。

## 4.2　网证管理客户端

网证管理客户端由硬件和软件组成。硬件形态可以是移动终端，或外接居民身份证件阅读器的计算机，或自助开通网证设备，或批量开通网证设备等；软件是运行在硬件上用于采集网证管理所需信息的应

用程序，该应用程序一般包含人脸图像采集控件。网证管理客户端具有网证开通、网证冻结、网证解冻、网证注销和网证口令重置等功能。

### 4.3 网证应用系统

网证应用系统由网证应用客户端和网证应用服务端组成。网证应用客户端由软、硬件组成，硬件形态一般是移动终端或计算机；软件是运行在硬件上用于采集网证下载和身份认证所需信息的应用程序，该应用程序一般包含人脸图像采集控件和信息获取控件。网证应用服务端由应用程序服务器、签名验签服务器和存储居民身份网络标识的数据存储设备组成。

### 4.4 居民身份网络认证服务系统

居民身份网络认证服务系统由网证管理服务接口、网证应用服务接口、签名验签、业务服务和数据存储等功能组成。其中业务服务包括网证管理、标识管理、网证验证、人脸验证、身份信息核验和身份信息验证等功能模块；数据存储包括网证和居民身份网络标识的存储。

## 5 业务功能

### 5.1 网证管理客户端

#### 5.1.1 网证开通

居民通过网证管理客户端的网证开通功能，在居民身份网络认证服务系统申请生成网证。开通网证时，居民需要出示居民身份证件，采集人脸图像，输入手机号码和设置网证口令，这些信息的提交可以根据网证管理客户端的界面提示进行操作。

#### 5.1.2 网证冻结

居民通过网证管理客户端的网证冻结功能，可以对在居民身份网络认证服务系统已经生成的网证进行冻结，冻结后此网证进入不可用状态，后续可以通过解冻操作恢复到可用状态。冻结网证时，网证客户端读取居民身份证件信息或读取网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。

#### 5.1.3 网证解冻

居民通过网证管理客户端的网证解冻功能，可以对在居民身份网络认证服务系统已经冻结的网证进行解冻，解冻后此网证恢复可用状态。解冻网证时，网证客户端读取居民身份证件信息或读取网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。

#### 5.1.4 网证注销

居民通过网证管理客户端的网证注销功能，可以对在居民身份网络认证服务系统已经生成的网证进行注销，注销后此网证直接失效，不可恢复。注销网证时，网证客户端读取居民身份证件信息或读取网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。

#### 5.1.5 网证口令重置

居民通过网证管理客户端的网证口令重置功能，可以对在居民身份网络认证服务系统已经生成的网证口令进行重置。网证口令重置时，网证客户端读取居民身份证件信息或读取网证信息、采集人脸图像和设置网证口令，提交到居民身份网络认证服务系统。

## 5.2 网证应用系统

### 5.2.1 网证应用客户端

网证应用客户端是网证应用系统面向居民用户的客户端，主要功能是接收居民的网证下载或身份认证请求，采集网证下载或身份认证所需的信息，并把相关信息转发给网证应用服务端；接收网证应用服务端转发的居民身份网络认证服务系统的返回结果，并展示给居民或引导居民进行网证应用系统的相关业务操作。

### 5.2.2 网证应用服务端

网证应用服务端是网证应用系统的后台服务，主要功能是对网证应用客户端发送的数据包按照居民身份网络认证服务系统服务接口要求进行组包和签名，并转发给居民身份网络认证服务系统；对居民身份网络认证服务系统返回的数据包进行验签和解析，并把结果转发至网证应用客户端。

## 5.3 居民身份网络认证服务系统

### 5.3.1 网证管理服务接口

网证管理服务接口主要与网证管理客户端进行数据交互，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。

### 5.3.2 网证应用服务接口

网证应用服务接口主要与网证应用系统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。

### 5.3.3 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。

### 5.3.4 业务服务

#### 5.3.4.1 网证管理

根据网证管理服务接口接收的功能请求，完成网证的生成、下载、注销、冻结、解冻和口令重置等功能。

#### 5.3.4.2 标识管理

完成居民身份网络标识的生成、查询、更新和删除等功能。

#### 5.3.4.3 网证验证

验证从网证应用服务接口接收的网证是否与居民身份网络认证服务系统存储的网证一致。

#### 5.3.4.4 人脸验证

验证从服务接口接收的人脸信息是否与居民身份网络认证服务系统存储的信息匹配。

#### 5.3.4.5 身份信息核验

在网证开通环节，核验从网证管理服务接口接收的身份证件信息是否与居民身份网络认证服务系统存储的信息一致。

#### 5.3.4.6 身份信息验证

在身份认证环节,验证从网证应用服务接口接收的除网证和人脸信息之外的信息是否与居民身份网络认证服务系统存储的信息相匹配。

### 5.3.5 数据存储

实现网证和居民身份网络标识等业务数据存储。

## 6 技术要求

### 6.1 一般要求

居民身份网络认证系统业务功能的具体技术要求应符合GA/T XXXX《居民身份网络认证 网络可信凭证和网络标识格式要求》、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.2《居民身份网络认证 认证服务 第2部分：服务接口要求》、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》、GA/T XXXX.4《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》、GA/T XXXX.5 《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》、GA/T XXXX.1《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》、GA/T XXXX.2《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》、GA/T XXXX.3《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》和GA/T XXXX.4《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》。

### 6.2 网证管理客户端

网证管理客户端技术要求如下：

a) 网证管理客户端集成的人脸图像采集控件应符合 GA/T XXXX.4《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》的要求；
b) 网证管理客户端硬件设备根据实际形态应满足：
   1) 居民身份证开通网证读卡器应符合 GA/T XXXX.1《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》的要求；
   2) 自助开通网证设备应符合 GA/T XXXX.2《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》的要求；
   3) 批量开通网证设备应符合 GA/T XXXX.3《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》的要求；
   4) 移动终端应支持网证的安全存储,应符合 GA/T XXXX.4《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》的要求。

### 6.3 网证应用系统

#### 6.3.1 网证应用客户端

网证应用客户端技术要求如下：

a) 网证应用客户端集成的信息获取控件应符合 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》的要求；
b) 网证应用客户端集成的人脸图像采集控件应符合 GA/T XXXX.4《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》的要求；

c) 网证应用客户端移动终端形态的设备应符合 GA/T XXXX.4《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》的要求。

#### 6.3.2 网证应用服务端

网证应用服务端技术要求如下：

a) 应通过网证应用服务接口与居民身份网络认证服务系统交互,实现网证下载和身份认证。接口协议应符合 GA/T XXXX.2《居民身份网络认证　认证服务　第 2 部分：服务接口要求》的要求；
b) 应提供存储区域,存储居民身份网络认证服务系统下发的居民身份网络标识。

### 6.4 居民身份网络认证服务系统

#### 6.4.1 网证管理服务接口

网证管理服务接口技术要求如下：

a) 应能实现协议的解析；
b) 应能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) 应能进行业务服务分发和调度。

#### 6.4.2 网证应用服务接口

网证应用服务接口技术要求如下：

a) 应能实现协议的解析；
b) 应能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) 应能进行业务服务分发和调度；
d) 应符合 GA/T XXXX.2《居民身份网络认证　认证服务　第 2 部分：服务接口要求》的要求。

#### 6.4.3 业务服务

业务服务技术要求如下：

a) 应提供网证管理、标识管理、网证验证、人脸验证、身份信息验证和核验等功能；
b) 人脸验证中的人脸比对引擎应符合 GA/T XXXX.5《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》的要求。

#### 6.4.4 数据存储

居民身份网络认证服务系统应实现网证和居民身份网络标识安全存储,应有灾备机制。

#### 6.4.5 系统安全

居民身份网络认证服务系统应符合GB/T 22239-2019和GM/T 0054-2018中的第三级安全要求。

# 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 32905-2016 信息安全技术 SM3密码杂凑算法
[8] GB/T 32915-2016 信息安全技术 二元序列随机性检测方法
[9] GB/T 33560-2017 信息安全技术 密码应用标识规范
[10]GB/T 35276-2017 信息安全技术 SM2密码算法使用规范
[11]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
[12]GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式规范
[13]GB/T 36322-2018 信息安全技术 密码设备应用接口规范
[14]GB/T 37092-2018 信息安全技术 密码模块安全要求
[15]GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范
[16]GA 490-2013 居民身份证机读信息规范
[17]GM/T 0008-2012 安全芯片密码检测准则
[18]GM/T 0014-2012 数字证书认证系统密码协议规范
[19]GM/T 0019-2012 通用密码服务接口规范
[20]GM/T 0024-2014 SSL VPN技术规范
[21]GM/T 0025-2014 SSL VPN网关产品规范
[22]GM/T 0026-2014 安全认证网关产品规范
[23]GM/T 0029-2014 签名验签服务器技术规范
[24]GM/T 0030-2014 服务器密码机技术规范
[25]GM/T 0032-2014 基于角色的授权与访问控制技术规范
[26]GM/T 0037-2014 证书认证系统检测规范
[27]GM/T 0038-2014 证书认证密钥管理系统检测规范
[28]ISO/IEC 29115:2013 Information technology - Security techniques - Entity authentication assurance framework（信息技术 安全技术 实体认证保证框架）
[29]《中华人民共和国居民身份证法》（2011年10月29日中华人民共和国主席令第五十一号）