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　网络可信凭证和网络标识格式要求

CTID online authentication—Format specifications for cyber trusted identity（CTID）and cyber identifier

（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、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。

本标准主要起草人：杨林、黄耀晖、吴国英、邱旭华、蔡子凡、谷晨、王俊峰。

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。

为了在网络空间进行身份认证，居民需要一个可以证明自己身份的文件和标识。为建立网络空间统一的身份证明和标识的规范，有效进行网络空间可信身份管理，特制定本标准。

居民身份网络认证　网络可信凭证和网络标识格式要求

1　范围

本标准规定了居民身份网络认证系统的居民身份网络可信凭证（网证）与网络标识的构成和数据结构。

本标准适用于居民身份网络认证相关系统的设计、开发、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 25069-2010　信息安全技术 术语

GB/T 32905-2016　信息安全技术 SM3密码杂凑算法

GB/T 35276-2017　信息安全技术 SM2密码算法使用规范

GA/T 543.6-2015　公安数据元（6）

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

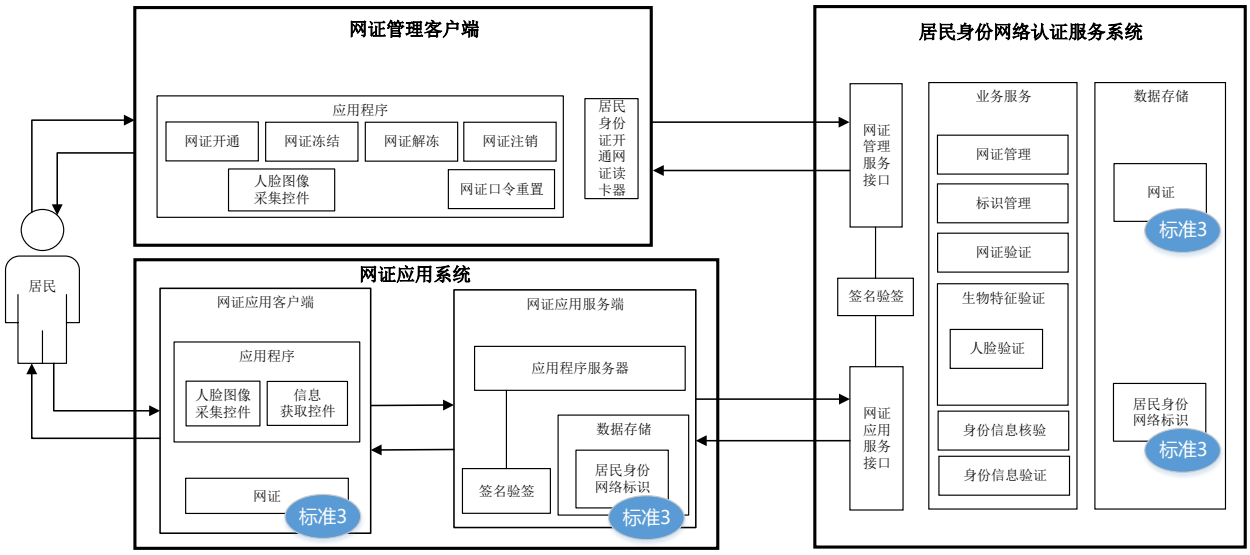
3　术语和定义

GB/T 25069-2010和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　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系统整体技术框架中，本标准规范的对象处于图1所示的“标准3”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
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

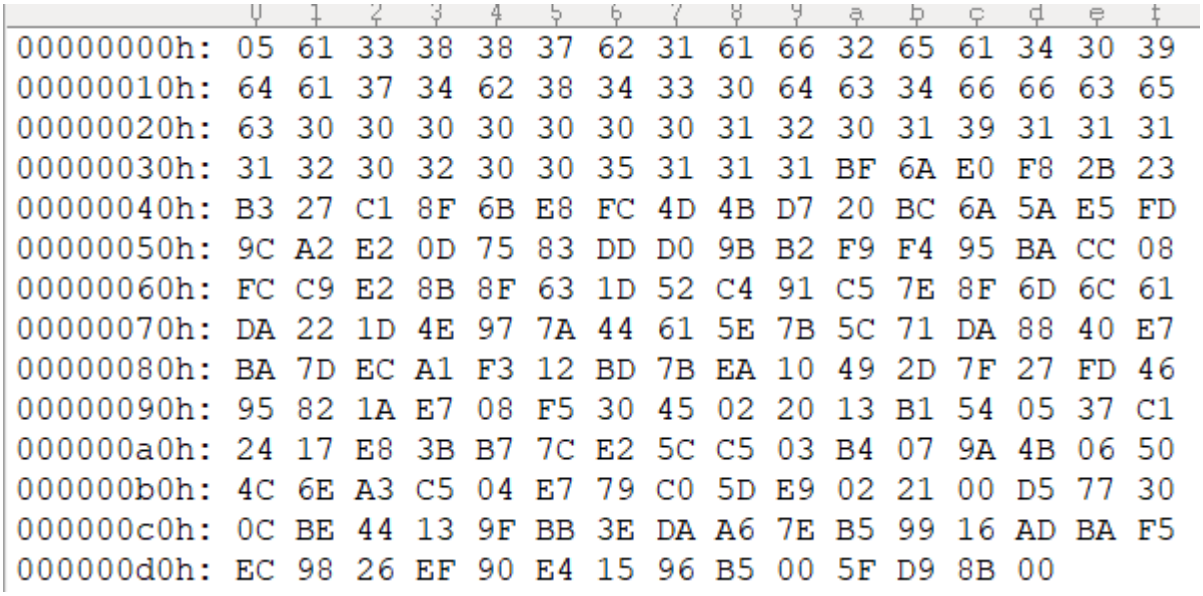
4.2　作用

在居民身份网络认证系统中，网络可信凭证（网证）是居民用于在网络空间证明自己身份的文件，居民身份网络标识是在网证应用系统中存储用于标识一个具体人的身份标识。网证和居民身份网络标识是贯穿居民身份网络认证系统的核心要素。在整个居民身份网络认证标准体系中，本标准是基于居民身份证件，建立网络空间用于身份证明和身份标识的规范，从而构建网络空间身份认证体系。

5　网络可信凭证

5.1　构成

网络可信凭证（网证）的信息由网证版本号、网证序列号、网证签发点编号、有效期起始日期、有效期截止日期、居民身份证件类别、网证主体要素、网证预留区和网证签名值构成，以二进制数存储。以十六进制展示的网证示例如图2所示。



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00000000h:	05	61	33	38	38	37	62	31	61	66	32	65	61	34	30	39
00000010h:	64	61	37	34	62	38	34	33	30	64	63	34	66	66	63	65
00000020h:	63	30	30	30	30	30	30	30	31	32	30	31	39	31	31	31
00000030h:	31	32	30	32	30	30	35	31	31	31	BF	6A	E0	F8	2B	23
00000040h:	B3	27	C1	8F	6B	E8	FC	4D	4B	D7	20	BC	6A	5A	E5	FD
00000050h:	9C	A2	E2	0D	75	83	DD	D0	9B	B2	F9	F4	95	BA	CC	08
00000060h:	FC	C9	E2	8B	8F	63	1D	52	C4	91	C5	7E	8F	6D	6C	61
00000070h:	DA	22	1D	4E	97	7A	44	61	5E	7B	5C	71	DA	88	40	E7
00000080h:	BA	7D	EC	A1	F3	12	BD	7B	EA	10	49	2D	7F	27	FD	46
00000090h:	95	82	1A	E7	08	F5	30	45	02	20	13	B1	54	05	37	C1
000000a0h:	24	17	E8	3B	B7	7C	E2	5C	C5	03	B4	07	9A	4B	06	50
000000b0h:	4C	6E	A3	C5	04	E7	79	C0	5D	E9	02	21	00	D5	77	30
000000c0h:	0C	BE	44	13	9F	BB	3E	DA	A6	7E	B5	99	16	AD	BA	F5
000000d0h:	EC	98	26	EF	90	E4	15	96	B5	00	5F	D9	8B	00		

图2　网证示例

5.2　数据结构

网证数据结构见表1。

表1　网证数据结构

序号	数据项名称	字节数	标识符	说明
1	网证版本号	1	WZBBH	表示网证数据结构的版本
2	网证序列号	32	WZXLH	随机生成的网证唯一序列号
3	网证签发点编号	8	WZQFDBH	网证签发点唯一编号，由居民身份网络认证平台生成
4	有效期起始日期	8	YXQQSRQ	符合 GA/T 543.6-2015 的 DE00612 规定
5	有效期截止日期	8	YXQJZRQ	符合 GA/T 543.6-2015 的 DE00611 规定
6	居民身份证件类别	1	JMSFZJLB	表示用于生成网证的居民身份证件类别，取值如下： 1-居民身份证； 2-出入境证件
7	网证主体要素	64	WZZTYS	由证件卡体序列号、公民身份号码或居民身份证件号码、姓名和随机数通过GB/T 32905-2016 SM3密码杂凑算法运算生成
8	网证预留区	28	WZYLQ	
9	网证签名值	72	WZQMZ	由前 8 个数据项通过 SM2 算法运算生成，格式符合 GB/T 35276-2017 要求的签名数据格式

6　网络标识

6.1　构成

居民身份网络标识的信息由网络标识版本号、网络标识编号、网络标识签发时间和网络标识签名值构成，以二进制数存储。以十六进制展示的网络标识示例如图3所示。

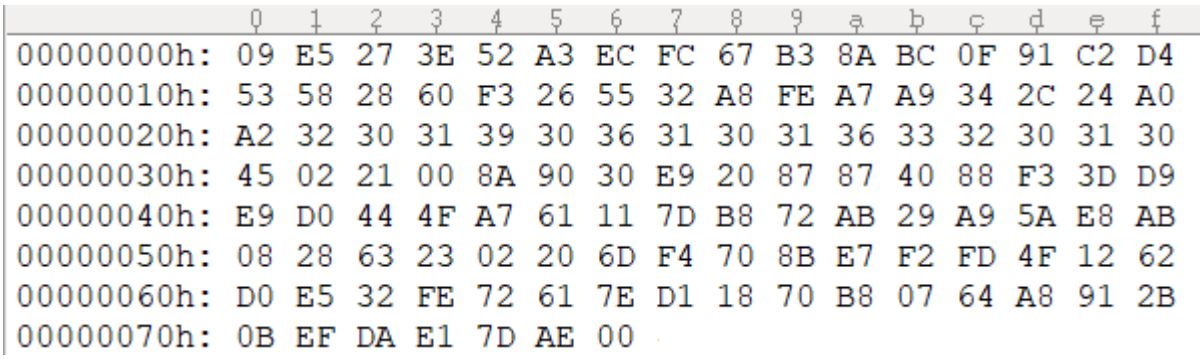


图3　网络标识示例

6.2　数据结构

居民身份网络标识数据结构见表2。

表2　居民身份网络标识数据结构

序号	数据项名称	字节数	标识符	说明
1	网络标识版本号	1	WLBSBBH	表示居民身份网络标识数据结构的版本
2	网络标识编号	32	WLBSBH	由公民身份号码或居民身份证件号码、网证应用系统服务机构编号、随机数通过GB/T 32905-2016 SM3密码杂凑算法运算生成
3	网络标识签发时间	14	WLBSQFSJ	由 GA/T 543.6-2015 中数据元 DE00554 “日期时间”派生
4	网络标识签名值	72	WLBSQMZ	由前 3 个数据项通过 SM2 算法运算生成，格式符合 GB/T 35276-2017 要求的签名数据格式

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] GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式
[3] 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
[4] GB/T 32915-2016 信息安全技术 二元序列随机性检测方法
[5] GB/T 33560-2017 信息安全技术 密码应用标识规范
[6] GA/T 490-2019 居民身份证机读信息规范
[7] GM/T 0008-2012 安全芯片密码检测准则