ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36632—2018

信息安全技术
公民网络电子身份标识格式规范

Information security technology—
Format specifications for citizen cyber electronic identity

2018-10-10 发布　　2019-05-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所、公安部十一局、公安部二十二局、中国科学院信息工程研究所、国家信息中心、北京数字认证股份有限公司、公安部信息安全等级保护评估中心、中国科学院软件研究所、上海格尔软件股份有限公司、普华诚信信息技术有限公司、金联汇通信息技术有限公司。

本标准主要起草人:胡传平、邹翔、陈兵、杨明慧、任军、周国勇、王慧元、刘丽敏、李新友、国强、张晏、傅大鹏、张妍、梁佐泉、谢超、田文晋、张立武、郑强、刘海龙、倪力舜、吴淼、李明。

信息安全技术
公民网络电子身份标识格式规范

1 范围

本标准规定了公民网络电子身份标识的组成及密钥对产生要求、格式要求和编码规则。

本标准适用于公民网络电子身份标识相关系统的设计、开发、测试、生产和应用。

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 18030 信息技术 中文编码字符集

GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 25069 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 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

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

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

公民网络电子身份标识 citizen cyber electronic identity

与公民真实身份具有一一对应关系，用于在线识别网络空间中公民真实身份的电子标识。

3.2

公民网络电子身份标识码 citizen cyber electronic identity code

使用公民真实身份有效证件的证件号码、公民姓名、证件类型代码和128个字节随机数的字串按特定的规则处理后得到的字符编码，由版本号、杂凑值和预留位三部分组成。

4 缩略语

下列缩略语适用于本文件。

ASN.1：抽象语法记法 I(abstract syntax notation one)

eID：公民网络电子身份标识(citizen cyber electronic identity)

HID：杂凑值编码(hash ID)

OID：对象标识符(object identifier)

5 组成及密钥对产生要求

5.1 公民网络电子身份标识组成

公民网络电子身份标识采用数字证书形式，由一对非对称密钥和含有其公钥及相关信息的数字证书组成。

5.2 公民网络电子身份标识非对称密钥对产生

公民网络电子身份标识的非对称密钥对由智能卡、智能密码钥匙等载体的安全芯片产生，包括公钥和私钥，其中私钥不可导出。

5.3 公民网络电子身份标识非对称密钥对产生算法

公民网络电子身份标识密钥对产生算法应符合 GB/T 32918.4—2016 的要求。

6 格式要求

6.1 概述

公民网络电子身份标识格式应符合表 1 的格式要求。

表 1 的各数据项按 GB/T 20518—2018 的规定进行定义。数据项的中文编码应符合 GB 18030 的要求，用 2 个到 4 个字节表示，其余字符用 1 个字节表示。数据交换时，各数据项按序号顺序排列。

表 1 公民网络电子身份标识格式

序号	数据项名称		数据类型	长度
1	版本号		整型	1 个字节
2	序列号		整型	不大于 20 个字节
3	签名算法		字符型	8 个字节
4	颁发机构	名称	字符型	16 个字节
		组织	字符型	18 个字节
		国家	字符型	2 个字节
		序号	字符型	6 个字节
5	有效期	生效日期	时间型	15 个字节
		失效日期	时间型	15 个字节
6	公民网络电子身份标识持有者信息	名称	字符型	48 个字节
		组织	字符型	18 个字节
		国家	字符型	2 个字节
7	公民网络电子身份标识持有者公钥信息		字符型	不小于 130 个字节

表 1（续）

序号	数据项名称		数据类型	长度
8	扩展项	颁发机构的密钥标识符	字符型	64 个字节
		标识持有者密钥标识符	字符型	64 个字节
		密钥用法	字符型	2 个字节
		密钥用法扩展	字符型	29 个字节
		证书策略	字符型	54 个字节
		撤销列表分发点	字符型	不大于 128 个字节
		浏览器证书类型	字符型	17 个字节
		颁发机构信息访问	字符型	62 个字节
9	签名值		字符型	不小于 64 个字节

6.2 版本号

版本号(version)是公民网络电子身份标识的数字证书版本。该数据项类型应为整型，长度为 1 个字节，其 ASN.1 的结构如下：

Version ::= INTEGER {v3(2)}

6.3 序列号

序列号(serialNumber)是公民网络电子身份标识的数字证书对应的唯一编号。该数据项应为长整型，长度不大于 20 个字节。其 ASN.1 的结构如下：

CertificateSerialNumber ::= INTEGER

6.4 签名算法

签名算法(signatureAlgorithm)是公民网络电子身份标识数字证书所使用的数字签名算法，应符合 GB/T 32918.2—2016 的要求。该数据项应为字符型，长度为 8 个字节。其 ASN.1 的结构如下：

Id-AlgorithmIdentifier OBJECT IDENTIFIER ::= {1.2.156.10197.1.501}

AlgorithmIdentifier ::= SEQUENCE {

algorithm OBJECT IDENTIFIER,

parameters ANY DEFINED BY algorithm OPTIONAL}

6.5 颁发机构

6.5.1 颁发机构组成

颁发机构(issuer)由颁发机构的名称、组织、国家的标识及颁发机构序号组成。

6.5.2 名称

该数据项应为字符型，长度不大于 16 个字节。其 ASN.1 的结构如下：

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

```
AttributeTypeAndValue ::= SEQUENCE {
                          type AttributeType,
                          value AttributeValue }
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
DirectoryString ::= CHOICE {
                    printableString PrintableString(SIZE(1..MAX)),
                    utf8String UTF8String(SIZE(1..MAX)) }
```

6.5.3 组织

该数据项应为字符型，长度为 18 个字节。值为颁发机构对应的统一社会信用代码或组织机构代码。

6.5.4 国家

该数据项应为字符型，长度为 2 个字节。值为中国的英文简称 CN。

6.5.5 序号

该数据项应为字符型，长度为 6 个字节。值为 000001～999999 之间的顺序编码。

6.6 有效期

有效期(validity)是一个时间段，由公民网络电子身份标识的生效日期和失效日期组成。该数据项长度为 30 个字节。生效日期和失效日期数据项均为时间型，长度均为 15 个字节。该时间段的值应为 5 年。其 ASN.1 的结构如下：

```
validity Validity
Validity ::= SEQUENCE {
         notBefore CertificateValidityDate,
         notAfter CertificateValidityDate }
CertificateValidityDate ::= CHOICE {
                        utcTime UTCTime,
                        generalTime GeneralizedTime }
```

6.7 公民网络电子身份标识持有者信息

6.7.1 持有者信息组成

持有者信息(subject)由持有者的名称、组织、国家的标识组成。其中持有者的名称由公民网络电子身份标识码表示。

6.7.2 名称

该数据项应为字符型，长度为 48 个字节。值为公民网络电子身份标识码，其 ASN.1 的结构如下：

```
RelativeDistinguishedName ::= SET OF AttributeTypeAndValue
```

```
AttributeTypeAndValue ::= SEQUENCE {
                          type AttributeType,
                          value AttributeValue }
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
DirectoryString ::= CHOICE {
                    printableString PrintableString(SIZE(1..MAX)),
                    utf8String UTF8String(SIZE(1..MAX)) }
```

6.7.3 组织

该数据项应为字符型，长度为 18 个字节。值为公民网络电子身份标识持有者对应的统一社会信用码或组织机构代码，可以为空。

6.7.4 国家

该数据项应为字符型，长度为 2 个字节。值为中国的英文简称 CN。

6.8 公民网络电子身份标识持有者公钥信息

持有者公钥信息(subjectPublicKeyInfo)包括公民网络电子身份标识的公钥及公钥算法的标识符，应符合 GB/T 32918.2—2016 的要求。该数据项应为字符型，长度不少于 130 个字节。其 ASN.1 的结构如下：

```
Id-subjectPublicKeyInfo OBJECT IDENTIFIER ::= {1.2.156.10197.1.301}
SubjectPublicKeyInfo ::= SEQUENCE {
                         algorithm AlgorithmIdentifier,
                         subjectPublicKey BIT STRING }
```

6.9 扩展项

6.9.1 扩展项组成

扩展项(extensions)定义的颁发机构密钥标识符、标识持有者密钥标识符、密钥用法、扩展密钥用途、证书策略、基本限制、撤销列表分发点、浏览器证书类型、颁发机构信息访问等扩展项的 OID 应符合 GB/T 20518—2018 中 5.2.3.2 的要求。其 ASN.1 的结构如下：

```
id-ce OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 29 }
```

6.9.2 颁发机构的密钥标识符

密钥标识符(authorityKeyIdentifier)用于验证在公民网络电子身份标识或撤销列表上签名的颁发机构公钥。该数据项为字符型，长度为 64 个字节。其 ASN.1 的结构如下：

```
id-ce-authorityKeyIdentifier OBJECTIDENTIFIER ::= {id-ce 35}
AuthorityKeyIdentifier ::= SEQUENCE {
                           keyIdentifier [0] KeyIdentifier OPTIONAL,
                           authorityCertIssuer [1] GeneralNames OPTIONAL,
```

```
                authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }
                (WITH COMPONENTS {…,authorityCertIssuer PRESENT,
                authorityCertSerialNumber PRESENT} |
                WITH COMPONENTS {…,authorityCertIssuer ABSENT,
                authorityCertSerialNumber ABSENT})
KeyIdentifier ::= OCTET STRING
```

6.9.3 标识持有者密钥标识符

持有者密钥标识符(subjectKeyIdentifier)用于标识公民网络电子身份标识持有者的公钥。该数据项为字符型,长度为 64 个字节。其 ASN.1 的结构如下:

```
id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= {id-ce 14}
SubjectKeyIdentifier ::= KeyIdentifier
```

6.9.4 密钥用法

密钥用法(keyUsage)用于标识公民网络电子身份标识中公钥的用法,包括但不限于数字签名和抗抵赖。该数据项为字符型,长度为 2 个字节。其 ASN.1 的结构如下:

```
id-ce-keyUsage OBJECT IDENTIFIER ::= {id-ce 15}
KeyUsage ::= BIT STRING {
        digitalSignature        (0),
        nonRepudiation          (1) }
```

6.9.5 密钥用法扩展

密钥用法扩展(extKeyUsage)用于标识公民网络电子身份标识中公钥的具体用途,包括但不限于客户端鉴别和电子邮件保护。该数据项为字符型,长度为 29 个字节。其 ASN.1 的结构如下:

```
id-ce-extKeyUsage OBJECT IDENTIFIER ::{id-ce 37}
ExtKeyUsageSyntax ::=SEQUENCE SIZE (1 ·· MAX) OF KeyPurposeId
KeyPurposeId::=OBJECT IDENTIFIER
```

6.9.6 证书策略

证书策略(certificatePolicies)用于标识公民网络电子身份标识发放所依据的策略及其应用目的。该数据项为字符型,长度为 54 个字节。其 ASN.1 的结构如下:

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::= { id-ce 32 }
CertificatePolicies ::= SEQUENCE {
        critical BOOLEAN DEFAULT FALSE,
        extnValue OCTET STRING }
```

6.9.7 撤销列表分发点

撤销列表分发点(CRLDistributionPoints)用于标识获得撤销列表信息的分发点序列。分发点应包含证书序列号,撤销时间,撤销列表存储的一个 X.500 或目录服务项对应的名称,宜包含撤销列表分发

点、颁发机构、撤销原因。该数据项应为字符型，长度不大于 128 个字节。其 ASN.1 的结构如下：

```
id-ce-CRLDistributionPoints OBJECT IDENTIFIER ::= { id-ce 31 }
CRLDistributionPoints ::= SEQUENCE {
                          critical BOOLEAN DEFAULT FALSE,
                          extnValue OCTET STRING }
```

6.9.8 浏览器证书类型

浏览器证书类型(browserCertType)用于标识公民网络电子身份标识所支持的浏览器证书类型。该数据项为字符型，长度为 17 个字节。其 ASN.1 的结构如下：

```
Id-ce-browserCertTypeIdentifier OBJECT IDENTIFIER ::= {2.16.840.1.113730.1.1}
BrowserCertTypeIdentifier ::= SEQUENCE {
                              critical BOOLEAN DEFAULT FALSE,
                              extnValue OCTET STRING }
```

6.9.9 颁发机构信息访问

颁发机构信息访问(authorityInfoAccess)用于标识公民网络电子身份标识颁发机构信息。该数据项为字符型，长度为 62 个字节。其 ASN.1 的结构如下：

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }
AuthorityInfoAccess ::= SEQUENCE {
        critical BOOLEAN DEFAULT FALSE,
        extnValue OCTET STRING }
```

6.10 签名值

签名值(signatureValue)用于标识公民网络电子身份标识颁发机构对公民网络电子身份标识的签名内容。该数据项为字符型，长度至少为 64 个字节。其 ASN.1 的结构如下：

```
Id-AlgorithmIdentifier OBJECT IDENTIFIER ::= {1.2.156.10197.1.501}
AlgorithmIdentifier ::= SEQUENCE {
                        algorithm OBJECT IDENTIFIER,
                        parameters ANY DEFINED BY algorithm OPTIONAL }
```

7 编码规则

7.1 编码格式

公民网络电子身份标识码共 48 个字节，由版本号、杂凑值和预留位三部分组成：

a) 第 1 个字节表示版本号，记为 eID_version；

b) 第 2 个至第 45 个字节表示杂凑值，记为 HID；

c) 第 46 个至第 48 个字节表示预留位，记为 eID_code_rvb。

7.2 HID 计算方法

HID 为字符串，计算方法如下：

$HID = Base_{64}[(SM3)[IDnumber|name|type|random\_hash]]$

其中“|”含义表示字符串连接。

IDnumber、name、type 和 random_hash 分别是有效证件的证件号码、公民姓名、证件类型代码和 128 个字节随机数的字串。证件类型代码见表 2。将 IDnumber、name、type、random_hash 依次顺序连接，采用符合 GB/T 32905—2016 要求的算法进行杂凑运算得出的二进制信息的 Base64 编码，共 44 个字节。

表 2　证件类型代码

证件类型代码	数据类型	证件名称
01	二进制	身份证
10	二进制	临时身份证

参 考 文 献

[1] GB/T 2260—2007 中华人民共和国行政区划代码

[2] GB/T 2659—2000 世界各国和地区名称代码

[3] GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第1部分:基本记法规范

[4] GB/T 16262.2—2006 信息技术 抽象语法记法一(ASN.1) 第2部分:信息客体规范

[5] GB/T 16262.3—2006 信息技术 抽象语法记法一(ASN.1) 第3部分:约束规范

[6] GB/T 16262.4—2006 信息技术 抽象语法记法一(ASN.1) 第4部分:ASN.1规范的参数化

[7] GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架

[8] 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

[9] 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

[10] RFC 2045 Multipurpose Internet Mail Extensions(MIME) Part One: Format of Internet Message Bodies