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、吴森、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)