ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36629.1—2018

信息安全技术 公民网络电子身份标识安全技术要求 第1部分:读写机具安全技术要求

**Information security technology—
Security technique requirements for citizen cyber electronic identity—
Part 1:Security technique requirements for reader**

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

GB/T 36629《信息安全技术　公民网络电子身份标识安全技术要求》分为以下部分：

——第1部分：读写机具安全技术要求；

——第2部分：载体安全技术要求；

——第3部分：验证服务消息及其处理规则。

本部分为GB/T 36629的第1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。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：公安部第三研究所、中国科学院软件研究所、国防科学技术大学、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、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。

本部分主要起草人：胡传平、邹翔、陈兵、杨明慧、贾焰、张立武、刘丽敏、李新友、国强、张晏、傅大鹏、张妍、梁佐泉、谢超、田文晋、郑强、刘海龙、倪力舜、胥怡心、夏丽娟、周斌、张严。

信息安全技术
公民网络电子身份标识安全技术要求
第1部分:读写机具安全技术要求

1 范围

GB/T 36629的本部分规定了公民网络电子身份标识读写机具的基本安全要求、数据初始化安全要求、密码应用管理安全要求和密码应用服务安全要求。

本部分适用于公民网络电子身份标识读写机具的设计、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/T 16649.3—2006 识别卡 带触点的集成电路卡 第3部分:电信号和传输协议

GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

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

GB/T 36632—2018 信息安全技术 公民网络电子身份标识格式规范

ISO/IEC 14443.4:2016 识别卡 非接触式集成电路卡 邻近卡 第4部分:传输协议(Identification cards—Contactless integrated circuit cards—Proximity cards—Part 4:Transmission protocol)

3 术语和定义

GB/T 36632—2018界定的以及下列术语和定义适用于本文件。

3.1

读写机具 reader

能够读写承载于智能卡、智能密码钥匙等载体中公民网络电子身份标识相关信息的机具。

3.2

读写机具安全模块 secure element of reader

读写机具内部的核心硬件电路安全组件。

3.3

读写机具数字证书 certificate of reader

用于标识读写机具身份的数字证书。

3.4

密码应用管理 cryptographic application management

用于对读写机具安全模块上的密钥进行生成、存储、导入、导出、更新的操作,并对读写机具数字证