



中华人民共和国国家标准

GB/T 36629.2—2018

信息安全技术 公民网络电子身份标识安全技术要求 第 2 部分：载体安全技术要求

Information security technology—
Security technique requirements for citizen cyber electronic identity—
Part 2: Security technique requirements of carrier

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	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 载体基本安全要求	2
5.1 概述	2
5.2 芯片	3
5.3 芯片操作系统	3
5.4 安全域	3
5.5 公民网络电子身份标识应用	4
6 芯片操作系统的应用安全要求	4
6.1 应用安全环境	4
6.2 应用间隔离	4
6.3 应用维护管理	4
6.4 文件系统和传输保护机制	4
7 载体密码应用管理安全技术要求	4
7.1 载体密钥管理	4
7.2 载体数字证书管理安全技术要求	6
8 载体密码应用服务安全技术要求	6
8.1 数字签名服务	6
8.2 签名 PIN 码服务	6
8.3 身份鉴别服务	6
附录 A (规范性附录) 文件系统和传输保护机制	7
参考文献	9

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2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2部分：载体安全技术要求

1 范围

GB/T 36629 的本部分规定了公民网络电子身份标识载体基本安全要求、芯片操作系统和应用安全要求、载体密钥应用管理安全技术要求和载体密码应用服务安全技术要求。

本部分适用于公民网络电子身份标识载体的设计、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 16649.4—2010 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令

GB/T 16649.6—2001 识别卡 带触点的集成电路卡 第6部分：行业间数据元

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 22186 信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求

GB/T 25069 信息安全技术 术语

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 20518—2018 信息安全技术 公民网络电子身份标识格式规范

GM/T 0008—2012 安全芯片密码检测准则

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 25069 和 GB/T 20518—2018 界定的以及下列术语和定义适用于本文件。

3.1

载体 carrier

用于承载公民网络电子身份标识的介质。

注：包括智能密码钥匙、智能芯片卡等形态。

3.2

载体数字证书 carrier certificate

颁发给载体的数字证书。