ICS 35.240.15
L 80

中华人民共和国国家标准

GB/T 35788—2017

机动车电子标识安全技术要求

Security technical requirement for the electronic identification of motor vehicles

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

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。

本标准由中华人民共和国公安部提出并归口。

本标准起草单位：公安部交通管理科学研究所、中国电子技术标准化研究院、北京中电华大电子设计有限责任公司、上海坤锐电子科技有限公司、国家射频识别产品质量监督检验中心。

本标准主要起草人：蔡岗、黄金、方万胜、宋继伟、梁浩、李志敏、李强、林万华、吴伟鸿、李坤。

机动车电子标识安全技术要求

1 范围

本标准规定了机动车电子标识安全的一般要求和生存周期安全。

本标准适用于机动车电子标识的设计、生产、试验和应用。

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 35789.1—2017 机动车电子标识通用规范 第1部分：汽车

GM/T 0035.1—2014 射频识别系统密码应用技术要求 第1部分：密码安全保护框架及安全级别

GM/T 0035.5 射频识别系统密码应用技术要求 第5部分：密钥管理技术要求

3 术语和定义

GB/T 35789.1—2017 界定的以及下列术语和定义适用于本文件。

3.1

身份鉴别 identity authentication

确认机动车电子标识或读写设备所声称身份的过程。

3.2

密文 ciphertext

加密后的数据。

[GM/Z 0001—2013，定义 2.60]

3.3

密钥 key

控制密码算法运算的关键信息或参数。

[GM/Z 0001—2013，定义 2.63]

3.4

初始密钥 initial key

机动车电子标识生产时写入的用于与读写设备之间进行身份鉴别的关键信息或参数。

3.5

初始化 initialization

由发行机构按规定将初始信息和密钥写入机动车电子标识的过程。

3.6

个性化 personalization

按规定将机动车登记信息写入机动车电子标识的过程。

4 一般要求

4.1 安全等级

安全等级应符合 GM/T 0035.1—2014 中 6.2.2 的要求。

4.2 密码算法

密码算法应使用国家密码管理部门认可的密码算法。

4.3 密钥

4.3.1 密钥长度为 128 位。存储在机动车电子标识内的密钥不应被读出。

4.3.2 密钥管理应符合以下要求：

a) 密钥的生成、分散、分发、注入、存储、备份、验证、更新、销毁和使用应符合 GM/T 0035.5 要求；

b) 芯片标识符区和机动车登记信息区的访问密钥由公安机关授权的机构负责管理；

c) 用户区的访问密钥由应用行业主管部门负责管理。

4.4 身份鉴别

应使用密码算法实现对读写设备身份的真实性鉴别。机动车电子标识与读写设备应进行双向身份鉴别，机动车电子标识不应响应读写设备的非授权访问命令。

4.5 机密性

机动车登记信息区信息应加密保护，用户区信息宜加密保护，并由授权的读写设备写入到指定存储区。

4.6 安全访问控制

应使用身份鉴别和口令验证安全机制对各存储分区进行访问权限控制。访问控制权限见表 1。

表 1 访问控制权限

存储分区	数据读取	数据写入
芯片标识符区	身份鉴别	不可写
机动车登记信息区	身份鉴别、口令验证	身份鉴别、口令验证
用户区	身份鉴别、口令验证	身份鉴别、口令验证
安全区	不可读	身份鉴别、口令验证

5 生存周期安全

5.1 生产

机动车电子标识生产应符合以下要求：

a) 芯片标识符在芯片生产过程中按 GB/T 35789.1—2017 中 4.1.4 的规则写入，写入后不可更改；

b) 芯片制造商应建立芯片标识符管理机制，确保芯片标识符的唯一性；

c) 机动车电子标识出厂前应写入初始密钥，初始密钥的传输应建立安全渠道。初始密钥的生成和更新方式由国家机动车登记主管部门与芯片制造商共同约定。

5.2 初始化

由国家机动车登记主管部门向机动车电子标识写入密钥、机动车登记信息区读/写口令，以及各用户区读/写初始口令。

5.3 个性化

由公安机关车辆管理部门向机动车电子标识的机动车登记信息区写入机动车登记信息，并在全国公安交通管理信息系统中记录核发的芯片标识符和标识序列号等信息。

5.4 使用

5.4.1 初始安装

机动车电子标识完成个性化和初始安装后，公安机关车辆管理部门应使用读写设备对机动车电子标识中存储的机动车登记信息进行验证。

5.4.2 更换

机动车电子标识损坏、灭失后应更换。按5.3和5.4.1的要求完成机动车电子标识个性化和验证工作，并在全国公安交通管理信息系统中标注原机动车电子标识作废。

5.4.3 信息读取

由应用行业主管部门授权的读写设备，经双向身份鉴别后，读取指定用户区的信息。

5.4.4 行业应用信息写入

由应用行业主管部门向对应的用户区写入更新后的口令和应用信息并进行验证。

5.4.5 信息更新

由应用行业主管部门授权的读写设备，经双向身份鉴别后，将更新信息以密文或明文方式写入指定用户区。

5.4.6 口令更新

应用行业主管部门应建立行业密钥管理体系，制定使用规范，并负责指定用户区读口令和写口令的更新。

5.5 报废

机动车报废时，应将机动车电子标识拆除后物理销毁，并在全国公安交通管理信息系统中标注该机动车电子标识作废。

参 考 文 献

[1] GM/Z 0001—2013 密码术语