ICS 35.240.15
L 80

中华人民共和国国家标准

GB/T 35787—2017

机动车电子标识读写设备安全技术要求

Security technical requirement for the read-write equipment of 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

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　一般要求 …… 1
5.1　通信安全要求 …… 1
5.2　基本结构 …… 1
5.3　密码算法 …… 2
5.4　密钥管理 …… 2
5.5　机密性 …… 2
5.6　完整性 …… 2
5.7　抗抵赖 …… 2
5.8　身份鉴别 …… 2
5.9　访问控制 …… 3
5.10　审计记录 …… 3
6　生产和报废处置 …… 3
6.1　生产 …… 3
6.2　报废处置 …… 3

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、睿芯联科(北京)电子科技有限公司、国家射频识别产品质量监督检验中心、国家道路交通安全产品质量监督检验中心。

本标准主要起草人：刘东波、黄金、胡家彬、徐敏杰、方万胜、高林、管超、李卓凡、杨勇、戴佳。

机动车电子标识读写设备安全技术要求

1 范围

本标准规定了机动车电子标识读写设备安全的一般要求、生产和报废处置。

本标准适用于机动车电子标识读写设备及应用系统的设计、开发、试验及应用。

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 0024 SSL VPN 技术规范

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

安全模块 security module

嵌入在读写设备内，为读写设备提供密码运算功能的部件。

4 缩略语

下列缩略语适用于本文件。

PSAM：终端安全模块(Purchase Secure Access Module)

SSL：安全套接层(Secure Sockets Layer)

VPN：虚拟专用网络(Virtual Private Network)

5 一般要求

5.1 通信安全要求

读写设备与机动车电子标识间的通信应满足 GM/T 0035.1—2014 中 6.2.2 的要求。

5.2 基本结构

读写设备中的读写单元包括通信模块、安全模块、处理器模块和射频模块，基本结构见图1。各模块功能如下：

a) 通信模块负责读写设备与应用系统之间的通信；