ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37985—2019

机动车电子标识密钥管理系统技术要求

Technical requirements for key management system for the electronic identification of motor vehicles

2019-08-30 发布　　2020-03-01 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 …… 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 …… 2
5　一般要求 …… 2
5.1　系统架构 …… 2
5.2　安全保护等级 …… 2
5.3　运行环境 …… 2
6　密钥管理和基本功能 …… 2
6.1　密钥管理 …… 2
6.2　基本功能 …… 4
附录A（规范性附录）　对称密钥分类 …… 5
附录B（规范性附录）　非对称密钥分类 …… 6

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、航天信息股份有限公司、华大半导体有限公司、天津中兴智联科技有限公司。

本标准主要起草人：王长君、黄金、王军华、方万胜、金涛、张科伟、马纪丰、杨益起。

机动车电子标识密钥管理系统技术要求

1 范围

本标准规定了机动车电子标识密钥管理系统的一般要求、密钥管理和基本功能。

本标准适用于机动车电子标识密钥管理系统的开发、测试、建设和使用。

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 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 35789.1—2017 机动车电子标识通用规范 第1部分：汽车

GM/T 0002 SM4分组密码算法

GM/T 0035.5—2014 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

机动车电子标识密钥管理系统 key management system for the electronic identification of motor vehicles

对机动车电子标识和读写设备的各类密钥进行管理的信息系统。

3.2

初始根密钥 original derivation key

用于生成根密钥的密钥。

3.3

根密钥 derivation key

用于生成身份鉴别和灭活口令等密钥的密钥。

3.4

出厂密钥 initialization key

机动车电子标识出厂时预置的密钥。

3.5

私钥 private key

非对称密码算法中不可以公开的密钥。

3.6

公钥 public key

非对称密码算法中可以公开的密钥。