GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 37985-2019

Technical Requirements for Key Management System for the Electronic Identification of Motor Vehicles

机动车电子标识密钥管理系统技术要求

Issued on: August 30, 2019 **Implemented on: March 1, 2020**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Technical Requirements for Key Management System for the Electronic Identification of Motor Vehicles

1 Scope

This Standard stipulates the general requirements, key management and basic functions of key management system for the electronic identification of motor vehicles.

This Standard is applicable to the development, testing, construction and application of key management system for the electronic identification of motor vehicles.

2 Normative References

The following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 22239-2008 *Information Security Technology - Baseline for Classified Protection of Information System Security;*

GB/T 35789.1-2017 *General Specification for the Electronic Identification of Motor Vehicles - Part 1: Automobile;*

GM/T 0002 *SM4 Block Cipher Algorithm;*

GM/T 0035.5-2014 *Specifications of Cryptographic Application for RFID Systems - Part 5: Specification for Key Management*

3 Terms and Definitions

What is defined in GB/T 35789.1-2017, and the following terms and definitions are applicable to this document.

3.1 Key Management System for the Electronic Identification of Motor Vehicles

Key management system for the electronic identification of motor vehicles refers to an information system, which implements management of various keys of the electronic identification and read-write equipment of motor vehicles.

3.2 Original Derivation Key

a) Be operated in public security's information communication network;

b) Cryptographic machine shall adopt commercial cryptographic products authorized by national cipher management department.

6 Key Management and Basic Functions

6.1 Key Management

6.1.1 Management procedure

The procedure of key management: generation, dispersion, injection, distribution, storage, backup, verification, update, archiving and destruction shall comply with the requirements in GM/T 0035.5-2014.

6.1.2 Key system

6.1.2.1 Key management system for the electronic identification of motor vehicles adopts two types of key system, namely, symmetric and asymmetric.

6.1.2.2 Symmetric key is applied to the identity authentication, access control, confidentiality and integrity protection between read-write equipment and the electronic identification of motor vehicles.

6.1.2.3 Asymmetric key is mainly applied to identity authentication, access control, non-repudiation, confidentiality and integrity protection among cryptographic machine, read-write equipment and back-end server.

6.1.3 Symmetric key

6.1.3.1 Key management and classification

The management of symmetric key shall comply with the requirements in 5.1 in GM/T 0035.5-2014. The classification of symmetric key is shown in Table A.1 in Appendix A.

6.1.3.2 Key generation

Original derivation key shall be generated by the central key management system through cryptographic machine. The generation process shall record audit information.

6.1.3.3 Key dispersion

Key dispersion shall comply with the following requirements:

a) Data encryption derivation key of motor vehicle registration information area which is injected into the sub-central key management system is generated through the dispersion of original derivation key. Dispersion factor shall be key category code;

Key distribution process between the central and sub-central key management system shall comply with the following requirements:

a) In the export and import operation of key, cryptographic machine has a security protection mechanism;

b) Encrypt the key; transmit it in the mode of ciphertext.

6.1.3.6 Key storage

Key storage shall comply with the following requirements:

a) All the derivation keys in the key management system are stored in cryptographic machine;

b) All the keys in read-write equipment are stored in security module; they cannot be exported;

c) Keys in the electronic identification of motor vehicles are stored in security zone and password-specific storage area of electronic identification of motor vehicles; they cannot be exported.

6.1.3.7 Key backup

Keys in the key management system of the electronic identification of motor vehicles shall comply with the following requirements:

a) Encrypt keys to be backed up; backup then in mediums like disk and intelligent IC card;

b) Separate key backup into multiple parts, which shall be respectively stored by different personnel;

c) Keys used for encryption key backup are stored in mediums like intelligent IC card and intelligent password key. They are also separated into multiple parts, which are respectively stored by different personnel.

6.1.3.8 Key verification

The integrity of keys and backup keys stored in the key management system of the electronic identification of motor vehicles shall be regularly verified.

6.1.3.9 Key update, archiving and destruction

Key update, archiving and destruction of the key management system of the electronic identification of motor vehicles shall comply with the following requirements:

a) It shall be able to support and manage multiple versions of original derivation key;

partitional write password, etc.; write into the security module of the read-write equipment.

f) Initialization of electronic identification of motor vehicles. Adopt the dispersion of original derivation keys to generate keys, such as: identity authentication, inactivation password, locking password, partitional read password and partitional write password, etc.; inject into the electronic identification of motor vehicles.

g) Cryptographic machine management, including switch between main cryptographic machine and backup cryptographic machine, work status query and cryptographic machine network settings, etc.

h) System user management, including adding new users, deleting users and setting users' operating permission, etc.

i) System log management, including log query, log backup and abnormal operating alarm, etc.

j) Remote supervision, including supervision of the operating status of the sub-central key management system.

6.2.2 Sub-central key management system

Sub-central key management system shall be equipped with the following functions:

a) Key management, including key backup, verification, update and destruction, etc.

b) Secure key import, including secure important of derivation keys, such as: identity authentication, inactivation password, locking password, partitional read password, partitional write password and partitional data encryption.

c) Data encryption and decryption service, including encryption and decryption service of data in the user area of the electronic identification of motor vehicles.

d) Cryptographic machine management, including switch between main cryptographic machine and backup cryptographic machine, work status query and cryptographic machine network settings, etc.

e) System user management, including adding new users, deleting users and setting users' operating permission, etc.

f) System log management, including log query, log backup and abnormal operating alarm, etc.

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------