ICS 03.220.20;35.240.60
R 07

中华人民共和国国家标准

GB/T 37376—2019

交通运输　数字证书格式

Transportation—Digital certificate format

2019-05-10 发布　　2019-12-01 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
引言 …… Ⅱ
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　证书分类 …… 2
6　数字证书格式 …… 2
附录 A（资料性附录）　ITS 设备证书格式示例 …… 10
附录 B（资料性附录）　证书撤销列表格式示例 …… 12
参考文献 …… 14

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国智能运输系统标准化技术委员会(SAC/TC 268)提出并归口。

本标准起草单位:交通运输部公路科学研究院、北京中交国通智能交通系统技术有限公司、中关村中交国通智能交通产业联盟、国家计算机网络与信息安全管理中心、北京信息科技大学、恒安嘉新(北京)科技股份公司、北京航空航天大学。

本标准主要起草人:梅新明、周洲、孙婧、王立岩、武俊峰、宋向辉、陈晓光、刘鸿伟、王永建、赵童、吴秋新、王云鹏、余贵珍。

引　言

本标准在国家对数字证书分类的基础上，结合交通运输信息系统各类应用场景，重点考虑了智能交通系统应用中，各类数据安全服务对数字证书长度、运算效率等方面的要求，对ITS设备证书的格式进行了规范化定义。

本标准凡涉及密码算法相关内容，均考虑了国产密码算法的应用与实现。

交通运输　数字证书格式

1　范围

本标准规定了交通运输信息系统中数字证书分类和数字证书格式。

本标准适用于交通运输信息系统中与数字证书应用相关的软硬件系统设计、研发及测试。

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 25069—2010　信息安全技术　术语

GM/T 0015　基于 SM2 密码算法的数字证书格式规范

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

智能运输系统　intelligent transport systems；ITS

在较完善的交通基础设施之上，将先进的科学技术(信息技术、计算机技术、数据通信技术、传感器技术、电子控制技术、自动控制理论、运筹学、人工智能等)有效地综合运用于交通运输、服务控制和车辆制造，加强车辆、道路、使用者三者之间的联系，从而形成一种保障安全、提高效率、改善环境、节约能源的综合运输系统。

3.2

合作式智能运输系统　cooperative ITS

通过人、车、路信息交互，实现车辆和基础设施之间、车辆与车辆、车辆与人之间的智能协同与配合的一种智能运输系统。

3.3

数字证书　digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构(CA)进行数字签名的一个可信的数字化文件。

[GB/T 20518—2018，定义 3.7]

3.4

ITS 设备证书　ITS device certificate

面向智能运输系统中的车载单元、路侧单元和移动终端等发放的具有特定格式的证书文件。

3.5

SM2 密码算法　SM2 algorithm

一种椭圆曲线密码算法，密钥长度为 256 比特。