ICS 03.220.20;35.240.60
R 07

中华人民共和国国家标准

GB/T 37374—2019

智能交通　数字证书应用接口规范

Intelligent transport—Digital certificate application interface

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
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　数字证书应用接口 …… 2
6　安全消息语法 …… 6
附录 A（资料性附录）　合作式 ITS 安全签名消息示例 …… 14
附录 B（资料性附录）　合作式 ITS 安全加密消息示例 …… 16
参考文献 …… 18

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。

智能交通　数字证书应用接口规范

1　范围

本标准规定了智能运输系统中的数字证书应用接口和安全消息语法。

本标准适用于智能运输系统中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 0010　SM2 密码算法加密签名消息语法规范

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

在较完善的交通基础设施上，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，从而形成的一种保障安全、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

由认证权威数字签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

[GB/T 20518—2006，定义 3.7]

3.4

SM2 算法　SM2 algorithm

一种椭圆曲线密码算法，密钥长度为 256 比特。

3.5

算法标识　algorithm identifier

用于标明算法机制的数字化信息。