国 家 标 准

《交通运输 数字证书格式》

（征求意见稿）

编制说明

《交通运输 数字证书格式》标准编制组

2017 年 7 月 31 日

目　录

一、工作简况.....1
二、编制原则和确定主要内容论据.....2
三、主要试验（或验证）的分析、技术经济认证或预期的经济效果.....5
四、与国际、国外同类标准水平的对比情况.....5
五、与有关的现行法律、法规和强制性标准的关系.....5
六、重大分歧意见的处理经过和依据.....5
七、标准作为强制性标准或推荐性标准的建议.....5
八、贯彻标准的要求和措施建议.....5
九、废止现行有关标准的建议.....6
十、其他应予说明的事项.....6

一、工作简况

1、任务来源

《交通运输 数字证书格式》列入了《2013 年国家标准制修订计划》，计划编号 20130077-T-469。

通过对交通运输行业深入的研究，对标准范围进行了重新界定，规定了交通运输行业中数字证书分类、基本元素以及合作式智能运输系统数字证书格式。

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，标准起草单位是交通运输部公路科学研究院。

2、协作单位

标准编制参加单位为北京中交国通智能交通系统技术有限公司、360 企业安全集团、恒安嘉新(北京)科技股份公司、国家互联网应急中心、北京信息科技大学。

3、主要工作过程

2011 年 10 月~2012 年 1 月，将《交通运输 数字证书格式》，作为交通运输部信息化课题《交通运输行业密钥管理与安全认证系统应用研究》的研究成果之一，纳入标准课题研究计划，成立了标准编写组。

2012 年 1 月~2012 年 7 月，对国家政策、相关标准进行搜集整理，先后到卫生部、水利部、民航空管局、中科院信息安全国家重点实验室进行专题调研。

2012 年 8 月~2014 年 1 月，确定标准编制技术方案后，先后在公路网出行报送系统、台湾海峡两岸航运网上行政许可系统、国家干线路网信息系统中进行验证性工作。

2014 年 1 月~2014 年 6 月，编制组起草了标准草稿，并对标准草稿进行详细研究讨论。

2014 年 7 月，完成标准征求意见稿的编写工作，通过网络、发函、会议等方式广泛征求意见。送达单位有中科院信息工程研究所、国家信息安全技术工程

研究中心、全国信息安全标准化技术委员会、国家密码行业标准化技术委员会、山东大学网络信息安全研究所、公安部第一研究所、山西、吉林数字证书认证中心、长春吉大正元信息技术股份有限公司等 20 余家。

2014 年 12 月，为确保标准先进性，经研究确定在标准原有内容基础上融合合作式智能运输系统和车联网概念，以满足相关内容要求。

2015 年 1 月~2017 年 6 月，与 360 企业安全集团、恒安嘉新(北京)科技股份公司、国家互联网应急中心、北京信息科技大学成立研究工作组，完成新版标准征求意见稿的编写工作。

4、主要起草人及其所做的工作

本标准主要起草人：王笑京、孟春雷、梅新明、周洲、孙婧、王立岩、武俊峰、宋向辉、王龑、郑新华、刘鸿伟、王永建、赵童、吴秋新。上述同志承担的主要工作如下：

——王笑京负责标准编制的组织、协调工作，进行标准需求分析、技术方案确定等工作。

——孟春雷、宋向辉、武俊峰、梅新明，负责数字证书分类及通用数字证书格式部分内容编写工作。

——周洲、王龑、郑新华、刘鸿伟、王永建、王立岩、赵童、孙婧、吴秋新负责 ITS 设备数字证书格式部分内容编写。

二、编制原则和确定主要内容论据

编制组收集了《交通运输信息化“十三五”发展规划》、《信息安全技术 信息系统通用安全技术要求》、《信息安全技术 公钥基础设施 数字证书格式》、《信息安全技术 公钥基础设施 时间戳规范》、《信息安全技术 信息系统安全等级保护基本要求》、《信息安全技术 基于互联网电子政务信息安全实施指南》、《信息安全技术 公钥基础设施安全支撑平台技术框架》、《基于 SM2 密码算法的数字证书格式规范》、《证书应用综合服务接口规范》、《时间戳接口规范》等标准。

编制组通过国内专题调研，广泛搜集资料等，对卫生部、水利部、人力资

源与社会保障部、民航空管局、中科院信息安全国家重点实验室等单位进行了调研，明确了《交通运输 数字证书格式》的编制内容、技术要求及相关规定。

1、标准编制原则

(1) 发展性原则

标准的制定既要符合我国国情，又要为发展留有充分的余地，以适合国内现状及发展。

(2) 先进性原则

数字证书系列标准是信息系统信任体系的核心，对于交通运输行业网络信任体系的建设与发展具有至关重要的意义，同时要与我国相关标准协调一致。

(3) 延续性原则

具有相对的稳定性，在一定的时期内保持标准的延续性。

2、标准的主要内容的说明

编制组对于数字证书格式标准的制定进行了充分的调研，收集了国内外有关技术资料、标准文本，分析了国际上交通运输相关安全标准的现状、发展趋势及产业化情况，结合中国的技术和标准情况，规定了交通运输系统中数字证书分类、交通运输系统数字证书格式。本标准按照 GB/T1.1 的格式要求编写。

(1) 关于标准名称

标准名称“交通运输 数字证书格式”，定位于对交通运输行业数字证书，定义了数字证书基本元素，说明了机构证书、人员证书、通用设备证书格式的引用标准，并对 ITS 设备证书专有格式进行了详细规范和描述。

(2) 规范性引用文件

近几年，国家颁布实施了一系列信息安全和密码技术相关的标准，其中非对称加密算法 SM2、摘要算法 SM3 和对称加密算法 SM4 是支撑加密机制的基础算法，

数字证书格式的定义和和应用的规范是本标准引用的依据。为此确定的规范性引用文件如下：

GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式

GB/T 25069-2010 信息安全技术 术语

GB/T 16262.1 信息技术 抽象语法记法-(ASN.1) 第 1 部分：基本记法规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范

(3) 术语和定义

针对交通运输数字证书格式新增定义术语包括：

ITS 设备证书 ITS device 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

(4) 缩略语

主要定义包括数字证书应用、密码应用、智能运输系统、编解码相关的缩略语。

AID：应用标识符（Application Identifier）

CA： 认证机构（Certificate Authority）

CRL：证书撤销列表（Certificate Revocation List）

ITS：智能运输系统（Intelligent transport system）

OID：对象标识符（Object Identifier）

SAE：美国汽车工程师学会(Society of Automotive Engineers)

UTC：协调世界时（Coordinated Universal Time）

(5) 证书分类

在国家对数字证书分类的基础上，结合交通运输信息系统应用场景，进一步细分为五类证书，分别是机构证书、公务人员证书、社会公众证书、设备证书和

ITS 设备证书。

(6) 数字证书格式

明确除 ITS 设备证书外，其他证书格式应符合 GM/T 0015-2012 标准要求。ITS 设备证书格式作为重点，在本标准中详细阐述。

三、主要试验（或验证）的分析、技术经济认证或预期的经济效果

本标准已先后在公路网出行报送系统、台海网上行政许可系统、国家干线路网信息系统中进行验证性工作，初步实现了智能运输系统信任体系的构建，切实保障了系统的应用安全。

本标准的制定，明确了交通运输领域数字证书格式的具体要求，对于密码技术及其相关产业在交通运输领域的落地发展，具有重要的指导意义。

四、与国际、国外同类标准水平的对比情况

参照工业和信息化部《GB/T 20518 信息安全技术 公钥基础设施 数字证书格式》结合交通运输领域应用情况进一步规范应用。

五、与有关的现行法律、法规和强制性标准的关系

遵循《交通运输信息化“十三五”发展规划》，符合交通运输部、工业和信息化部现行有效的政策法规及有关规定，协调好与相关标准的关系。以适用性、可操作性为目的，进行标准研究和编制。

六、重大分歧意见的处理经过和依据

目前没有。

七、标准作为强制性标准或推荐性标准的建议

编制组建议本标准制定为推荐性国家标准。

八、贯彻标准的要求和措施建议

1、开展标准宣贯培训

制定标准尽管重要，也只是标准化工作的基本前提，标准化工作的关键是标

准的贯彻实施，离开宣贯，再好的标准也不能产生任何社会和经济效益。

在全国智能运输系统标准化技术委员会的组织协调下，积极开展本标准的宣贯培训，使得业务人员、管理人员和技术人员及时了解、熟悉本标准，提高采标人员的标准应用水平，充分发挥本标准的规范和指导作用。

2、推进标准的有效应用

标准的有效应用和指导实践是标准制定工作的根本目的。

全国智能运输系统标准化技术委员会和标准编写组统筹规划和组织协调，开展标准在交通运输领域试点应用工作，验证标准的实用性，发现本标准在实际应用中存在的问题，以利于修订和完善标准，保障标准在应用中发挥有效作用，促进对标准成果和试点应用经验的宣传与推广，实现技术研发、实际应用与标准研制的有机互动。

因此，全国智能运输系统标准化技术委员会，将在交通运输部相关司局的指导下，做好标准研究、制定、宣贯、实施的全过程工作。

九、废止现行有关标准的建议

无。

十、其他应予说明的事项

无。