国 家 标 准

《智能交通 数字证书应用接口规范》

（征求意见稿）

编制说明

《智能交通 数字证书应用接口规范》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.....6
四、与国际、国外同类标准水平的对比情况.....6
五、与有关的现行法律、法规和强制性标准的关系.....6
六、重大分歧意见的处理经过和依据.....6
七、标准作为强制性标准或推荐性标准的建议.....6
八、贯彻标准的要求和措施建议.....7
九、废止现行有关标准的建议.....7
十、其他应予说明的事项.....7

一、工作简况

1、任务来源

《智能交通 数字证书应用接口规范》列入了《2011 年国家标准制修订计划》，计划编号 20111694-T-469。

通过对智能运输系统深入的研究，对智能运输系统中数字证书应用的安全消息的语法和数字证书应用接口进行了规范，同时对安全消息语法的基本元素格式进行了定义。

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《智能运输 数字证书应用接口规范》标准，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，负责数字证书应用接口部分内容编写工作。

——周洲、王龑、郑新华、刘鸿伟、王永建、王立岩、赵童、孙婧、吴秋新负责合作式 ITS 安全消息语法部分内容编写。

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《智能交通 数字证书应用接口规范》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应用接口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，分析了国际上智能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，对面向智能运输系统证书应用的统一服务接口进行了定义，同时定义了 ITS 设备证书环境下使用 SM2 密码算法的加密签名消息数据结构。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“智能交通 数字证书应用接口”，定位于智能运输系统中的数字证书应用接口和安全消息语法，适用于智能运输系统中数字证书应用相关的软硬件系统的设计、研发、测试及数字证书认证机构的运行、维护和管理。

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

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

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

GM/T 0020-2012 证书应用综合服务接口规范

(3) 术语和定义

针对智能交通数字证书应用接口规范新增定义术语包括：

智能运输系统 intelligent transport systems(ITS)。又称智能交通系统，是在较完善的交通基础设施之上，在先进的信息、通信、计算机、自动控制和系统集成等技术前提下，通过先进的交通信息采集与融合技术，交通对象交互以及智能化交通控制与管理等专有技术，加强载运工具载体和用户之间的联系，提高交通系统的运行效率，减少交通事故，降低环境污染，从而建立一个高效、便捷、安全、环保、舒适的综合交通运输体系。

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（V2I）、车辆与车辆（V2V）、车辆与人（V2P）之间的智能协同与配合的一种智能运输系统体系。

(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。

ASN.1：抽象语法标记（Abstract Syntax Notation One）

CA： 认证机构（Certificate Authority）

OER：八位字节编码规则（Octet Encoding Rules）

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）

UTC：协调世界时（Coordinated Universal Time）

(5) 数字证书应用接口

本部分定义在合作式智能交通、车联网等应用中，与数字证书相关的数据接口，这些接口包括获取版本号、消息签名与验证、消息加密与解密、消息信封等。

这些接口主要完成基于数字证书的密码应用，是为安全服务的基础。

(6) 安全消息语法

安全消息语法定义了智能交通系统中安全消息的数据结构，根据安全消息应用场景和系统的不同，划分为传统的安全消息和智能交通专用安全消息。传统的安全消息可遵照国家现有的相关标准定义使用，如 GM/T 0010。智能交通专用消息时结合传统安全消息的规定，为适应行业特色专门定义的消息结构，这种消息的数据结构更简单，复杂度更低、安全消息加解密的效率更高，更适合在交通无线通信领域中的应用。

智能交通安全消息在结构上划分为协议版本、头部字段、有效负载、尾部字段几部分，在标准中对每部分规定了详细的字段内容。其中有效负载是承载应用数据的关键部分，应用数据的加解密在这部分中完成，尾部字段是整个消息的数字签名，是确认消息发送主体、判断传输中未被篡改的重要标识。

(7) 基本元素格式

数据类型组成合作式智能交通系统数据结构的基本元素，这些元素类型在合作式智能交通系统的安全消息中使用。在本标准中使用 ASN.1 对数据结构和消息语法进行描述，采用八位字节编码规则(OER)对签名加密消息的各项信息进行编码。本节主要定义整型、32 位时间、64 位时间、3D 位置、8 字节哈希值、3 字

节哈希值、公钥算法、对称算法、加密密钥、公钥、加密的对称密钥、加密参数、签名者信息、接收者信息、签名等数据类型。

(8) 附录 合作式 ITS 安全消息示例

本部分提供一个合作式 ITS 安全消息的示例，给出一个安全消息的数据结构的具体实例，方便标准的使用者能通过这个实例分析安全消息的编码原理，更容易理解正文中的定义。

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

本标准规定了面向智能交通系统证书应用的统一服务接口，定义了签名加密消息的基本元素格式，同时定义了 ITS 设备证书环境下使用 SM2 密码算法的加密签名消息数据结构。

本标准的制定，明确了智能交通数字证书应用接口的具体要求，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

参照国家密码管理局《通用密码服务接口规范》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

无。

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。