ICS 03.220.20;35.240.60
CCS R 07

中华人民共和国国家标准

GB/T 37376—2024
代替 GB/T 37376—2019

交通运输 数字证书格式

Transportation—Digital certificate format

2024-08-23 发布　　2025-03-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 37376—2019《交通运输　数字证书格式》，与GB/T 37376—2019相比，除结构调整和编辑性改动外，主要技术变化如下：

a） 删除了智能运输系统、合作式智能运输系统的术语和定义（见2019年版的3.1、3.2）；

b） 更改了ITS设备证书、SM2密码算法的术语和定义（见3.2、3.3，2019年版的3.4、3.5）；

c） 增加了COER、CRACA、LA、SPDU、SSP等缩略语，删除了缩略语UTC（见第4章，2019年版的第4章）；

d） 更改了数字证书分类（见第5章，2019年版的第5章）；

e） 更改了数字证书通用格式要求（见6.1，2019年版的6.1）；

f） 更改了ITS数字证书基本元素的编码规则（见6.2.1.1，2019年版的6.2.1.1）；

g） 更改了基本数据类型、32位时间、地理有效区域、矩形区域、三维位置信息、纬度、经度、对称加密算法、签名的结构定义（见6.2.1.2、6.2.1.8、6.2.1.10、6.2.1.12、6.2.1.16、6.2.1.17、6.2.1.18、6.2.1.24、6.2.1.27，2019年版的6.2.1.2、6.2.1.9、6.2.1.10、6.2.1.12、6.2.1.15、6.2.1.16、6.2.1.17、6.2.1.6、6.2.2.7）；

h） 更改了“8字节哈希值”“摘要算法”“加密公钥”为“8字节杂凑值”“杂凑算法”“公钥加密密钥”，并更改了其结构定义（见6.2.1.5、6.2.1.7、6.2.1.23，2019年版的6.2.1.3、6.2.1.4、6.2.1.8）；

i） 增加了应用标识、3字节杂凑值、10字节杂凑值、64位时间、已识别区域、高程、CRL所属系列、加密密钥、对称加密密钥、特定算法的公钥加密密钥、256位椭圆曲线和256位SM2签名的结构定义（见6.2.1.3、6.2.1.4、6.2.1.6、6.2.1.9、6.2.1.14、6.2.1.19～6.2.1.22、6.2.1.25、6.2.1.26、6.2.1.28）；

j） 删除了椭圆曲线算法、签名公钥的结构定义（见2019年版的6.2.1.5、6.2.1.7）；

k） 更改了证书结构、签名者信息的结构定义（见6.2.2.1、6.2.2.7，2019年版的6.2.2.1、6.2.2.3）；将“版本”改为“证书版本”，并更改了其结构定义（见6.2.2.3，2019年版的6.2.2.2）；

l） 增加了证书基本结构、证书类型、显式证书、隐式证书、证书信息、证书持有者信息、链接数据、链接值、群组链接值、主机名称、有效期、持续时间、国家标识、国家和区域标识、国家和子区域标识、区域和子区域标识、证书持有者置信度、应用标识服务特定权限、服务特定权限、比特位图、应用标识集合权限、证书持有者权限、终端类型、应用标识服务特定权限区域、服务特定权限区域、比特位图服务特定权限区域、验证密钥指示、验证公钥的结构定义（见6.2.2.2、6.2.2.4～6.2.2.6、6.2.2.8～6.2.2.31）；

m） 删除了主题信息、主题属性、有效性限定的结构定义（见2019年版的6.2.2.4、6.2.2.5、6.2.2.6）；

n） 更改“证书撤销列表格式”为“ITS证书撤销列表”，并删除了证书撤销列表格式的结构定义（见6.3，2019年版的6.3）；

o） 增加了ITS CRL封装格式、ITS CRL内容、优先级信息、撤销证书信息、基于杂凑的撤销信息、撤销证书链接值信息、撤销批次信息、链接机构信息、撤销总数信息、个体链接数据、双链接机构CRL信息、单链接机构CRL信息、链接机构标识、链接种子的结构定义（见6.3.1～6.3.14）；

p） 增加了签名运算过程说明（见附录A）；

q） 更改了ITS证书示例（见附录B，2019年版的附录A）；

r） 增加了ITS CRL安全封装相关数据结构（见附录C）；

s） 更改了ITS CRL示例（见附录D，2019年版的附录B）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件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。

本文件起草单位：交通运输部公路科学研究所、北京中交国通智能交通系统技术有限公司、北京航空航天大学、华为技术有限公司、郑州信大捷安信息技术股份有限公司、中路高科交通科技集团有限公司。

本文件主要起草人：李斌、王立岩、王云鹏、刘鸿伟、汪林、梅新明、刘为华、潘凯、周吉祥、齐志峰、王佳宁、康亮、周洲、王小军、宋向辉、余贵珍、范晨歌、张玥、赵童、马岁、宫福军。

本文件于2019年首次发布，本次为第一次修订。

交通运输 数字证书格式

1 范围

本文件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的要求。

本文件适用于交通运输信息系统中与数字证书相关的软硬件系统设计、研发、测试及应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 2659.1 世界各国和地区及其行政区划名称代码 第1部分：国家和地区代码

GB/T 13000 信息技术 通用多八位编码字符集（UCS）

GB/T 16262（所有部分） 信息技术 抽象语法记法一(ASN.1)

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918.1 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

YD/T 3957—2021 基于LTE的车联网无线通信技术 安全证书管理系统技术要求

ISO/IEC 8825-7 信息技术 抽象语法记法编码规则 第7部分：八位位组编码规则（Information technology—ASN.1 encoding rules—Part 7: Specification of Octet Encoding Rules）

3 术语和定义

GB/T 25069、GB/T 32905、GB/T 32907、GB/T 32918.2界定的以及下列术语和定义适用于本文件。

3.1

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。

[来源：GB/T 20518—2018，3.7]

3.2

ITS证书 ITS certificate

面向智能运输系统中的车载单元、路侧单元、移动终端和运营服务提供商等发放的具有特定格式的数字证书。

3.3

SM2算法 SM2 algorithm

由GB/T 32918定义的一种椭圆曲线公钥密码算法。