ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/TXXXXX—XXXX

交通运输 数字证书格式

Transportation - Digital certificate format

（征求意见稿）

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这些专利的责任。

（本稿完成日期：2017-7-31）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

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/TC268)提出并归口。

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这些专利的责任。

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、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。

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。

交通运输 数字证书格式

1 范围

本标准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。

本标准适用于交通运输系统中数字证书应用相关的软硬件系统(包含合作式智能运输系统和车联网等应用）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

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 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

GB/T 25069界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 25069中的某些术语和定义。

3.1

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。

[GB/T 20839-2007，定义2.1]

3.2

合作式智能运输系统 cooperative ITS

合作式智能运输系统是由载运装备单元、基础设施单元、数据传输网络、网络管理控制平台、业务管理平台、网关设备等部分共同组成的信息管理、控制、分发的系统，可以向交通运输管理者、业务提供者和使用者提供服务和应用的综合性信息系统。

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。

3.4

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

3.5

证书撤销列表 certificate revocation list；CRL

CA对撤销的证书而签发的一个列表文件。

3.6

证书认证机构 certificate authority；CA

负责创建和分配证书，受到用户信任的权威机构。用户可以选择该机构为其创建密钥。

3.7

SM2算法 SM2 algorithm

一种椭圆曲线密码算法，密钥长度为256比特。

3.8

算法标识 algorithm identifier

用于标明算法机制的数字化信息。

4 缩略语

以下缩略语适用于本文件。

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

交通运输系统中数字证书的签发和管理包括以下五类证书：

a) 机构证书——面向交通运输系统内部机构或服务单位发放。

b) 公务人员证书——面向交通运输系统计算机终端用户发放（工作人员）。

c) 社会公众证书——面向交通运输系统计算机终端用户发放（外部用户）。

d) 设备证书——面向交通运输系统的服务器、终端设备等发放。
e) ITS 设备证书——面向交通运输系统中的车载单元、路侧单元和移动终端等发放。

6 数字证书格式

6.1 机构证书格式

机构证书格式应符合GM/T 0015-2012标准要求。

6.2 公务人员证书格式

人员证书格式应符合GM/T 0015-2012标准要求。

6.3 社会公众证书格式

人员证书格式应符合GM/T 0015-2012标准要求。

6.4 设备证书格式

通用设备证书格式应符合GM/T 0015-2012标准要求。

6.5 ITS 设备证书格式

6.5.1 基本元素说明

6.5.1.1 整型

```
The following atomic types are used in the data structure definitions:
下面的原子类型在数据结构定义中使用:
Uint3 ::= INTEGER (0..7)                                    -- (hex)          07
Uint8 ::= INTEGER (0..255)                                  -- (hex)          ff
Uint16 ::= INTEGER (0..65535)                               -- (hex)       ff ff
Uint32 ::= INTEGER (0..4294967295)                          -- (hex) ff ff ff ff
Uint64 ::= INTEGER (0..18446744073709551615) -- (hex) ff ff ff ff ff ff ff ff
IValue ::= Uint16
CrlSeries ::= Uint16
下面的八位字节字符串的同义词在数据结构定义中使用:
Opaque ::= OCTET STRING
下列结构用来阐明定义:
SequenceOfOctetString ::= SEQUENCE (SIZE (0..MAX)) OF
OCTET STRING (SIZE(0..MAX))
SequenceOfUint3 ::= SEQUENCE OF Uint3
SequenceOfUint8 ::= SEQUENCE OF Uint8
SequenceOfUint16 ::= SEQUENCE OF Uint16
```

6.5.1.2 公钥加密算法 PublicKeyAlgorithm

```
PublicKeyAlgorithm::= ENUMERATED {
```

```
    sgdsm3sm2                       (2),
    sgdsm2                          (3),
    ...
    }
```

本枚举表示基于公钥加密的算法。0、1、240~255之间的数值作为保留项。

6.5.1.3 对称加密算法 SymmetricAlgorithm

```
    SymmetricAlgorithm::= ENUMERATED {
        sgdsm4ecb                   (1),
        sgdsm4cbc                   (2),
        sgdsm4cfb                   (3),
        sgdsm4ofb                   (4),
        ...
    }
```

本枚举类型列举应支持的对称密码算法。

本枚举表示基于对称密钥加密的算法。0、240~255之间的数值作为保留项。

6.5.1.4 公钥 PublicKey

```
    PublicKey::= CHOICE{
        signKey OCTET STRING(SIZE(32)),
        encKey EncryptKey,
        ...
    }
    EncryptKey ::= SEQUENCE{
        supportedSymmAlg       SymmetricAlgorithm,
        signKey               OCTET STRING(SIZE(32))
    }
```

该结构表示一个公钥。SignKey表示一个签名密钥；EncKey表示一个加密密钥，它由一个签名密钥和指定的对称加密算法组成。

6.5.1.5 8字节哈希值 HashedId8

```
    HashedId8 ::= OCTET STRING (SIZE(8))
```

本哈希值用来识别证书等数据。这个数据结构包含另一个数据结构的散列。首先计算输入数据的SM3哈希值,然后从哈希值中取8个最低有效字节。最低的八个字节是32字节的散列的最后八个字节。

6.5.1.6 32位时间 Time32

```
    Time32 ::= Uint32
```

Time32是一个32位无符号整数，高位优先编码格式，自2004年1月1日UTC 00:00:00开始，给出国际原子时间的秒数。

6.5.1.7 区间 Duration

```
    Duration ::= Uint16
```

本区间采用uint16编码定义时间跨度。前3位比特定义了时间单位（见表1）。剩余13位应视为一个编码整体代表时间长度。

该结构定义了一个证书的有效时间。Uint16值期间,因为在单位用指定的选择。一年被认为是31556952秒，见表1。

表1　持续时间单元比特含义

比特	含义
000	秒
001	分钟（60秒）
010	小时（3600秒）
011	60小时 (216 000秒)
100	年(31 556 925秒)
101、110、111	未定义

6.5.1.8　地理有效区域　GeographicRegion

```
GeographicRegion ::= CHOICE {
    circularRegion          CircularRegion,
    rectangularRegion       SequenceOfRectangularRegion,
    polygonalRegion         PolygonalRegion,
    ...
}
SequenceOfRectangularRegion ::= SEQUENCE OF RectangularRegion
```

本项标识定义了证书应用地理区域，这些区域可以用来限制证书的有效性。

证书所有者所包含的范围有任何一部分在规定的范围以外即为无效。

6.5.1.9　圆形区域　CircularRegion

```
CircularRegion ::=SEQUENCE {
    center TwoDLocation,
    radius Uint16
}
```

本结构定义了一个圆形区域，该圆具有以米为单位的半径radius和中心center。指定的地区参考椭球体的表面上的所有点的距离中心点在参考椭球体小于或等于半径。点包含海拔组件被认为是在圆形区域内的水平投影参考椭球体位于该地区。

6.5.1.10　矩形区域　RectangularRegion

```
RectangularRegion ::=SEQUENCE {
    northWest TwoDLocation,
    southEast TwoDLocation
}
```

这个结构指定矩形由依次连接：(northWest.latitude, northWest.longitude), (southEast.latitude, northWest.longitude), (southEast.latitude, southEast.longitude), and

(northWest.latitude, southEast.longitude)。点由经度或纬度的等值线连接。点包含海拔组件被认为是矩形区域内的水平投影参考椭球体位于该地区。

6.5.1.11 多边形区域 PolygonalRegion

```
PolygonalRegion ::= SEQUENCE SIZE(3..MAX) OF TwoDLocation
```

这个数据结构定义了一个地区使用一系列不同的地理点,定义在参考椭球体的表面。通过连接指定的地区分它们出现的顺序,每一对分通过参考椭球体上的测地线连接。完成多边形通过连接最终指向第一点。允许的地区是多边形的内部及边界。

点包含海拔组件被认为是多边形区域内的水平投影参考椭球体位于该地区。

一个有效的PolygonalRegion包含至少三分。在有效PolygonalRegion,隐含线构成的多边形不相交。

6.5.1.12 2D 位置 TwoDLocation

```
TwoDLocation ::=SEQUENCE {
    latitude     Latitude,
    longitude   Longitude
}
```

这个数据结构用于定义区域用于证书的有效性。纬度和经度字段包含上面定义的纬度和经度。

注意:这个数据结构是一致的位置编码中使用SAE J2735[B20],除了为纬度值900 000 001(用于表明纬度不是可用)和1 800 000 001经度(用来表示经度没有可用)是无效的。

6.5.1.13 维度 Latitude

```
Latitude ::= NinetyDegreeInt
NinetyDegreeInt ::= INTEGER {
    min (-900000000),
    max (900000000),
    unknown (900000001)
} (-900000000..900000001)
KnownLatitude ::= NinetyDegreeInt (min..max)
-负90度到正90度，间隔为1微度。
UnknownLatitude ::= NinetyDegreeInt (unknown)
纬度字段包含一个整数编码，精度为1微度。
允许的纬度值范围从-900 000 000~ + 900 900 000。值900 000 001表明纬度是不可用的。
```

6.5.1.14 经度 Longitude

```
Longitude ::= OneEightyDegreeInt
OneEightyDegreeInt ::= INTEGER {
    min (-1799999999),
    max (1800000000),
    unknown (1800000001)
} (-1799999999..1800000001)
KnownLongitude ::= OneEightyDegreeInt (min..max)
UnknownLongitude ::= OneEightyDegreeInt (unknown)
经度字段包含一个整数编码，精度为1微度。
```

允许的经度值范围从-1 800 000 000~+1 800 000 000。值1 800 000 001表示经度是不可用的。

6.5.2 证书 Certificate

ITS设备数字证书即为合作式智能交通系统数字证书，基本数据结构如下：

```
Certificate  ::= SEQUENCE  {
    version                     Uint8,
    signerInfo                  SignerInfo,
    subjectInfo                 SubjectInfo,
    subjectAttributes           SubjectAttribute,
    validityRestrictions        ValidityRestriction,
    signature                   Signature
}
```

ITS设备数字证书示例参见附录A。

6.5.3 版本 Version

本项描述了证书的版本号。为符合当前文档该值应设为2。

6.5.4 签名者信息 SignerInfo

本项描述了证书签名者的信息。该项被定义为SignerInfo类型，其结构如下：

```
SignerInfo  ::= CHOICE {
    self                            NULL,
    certificateDigestWithSM3        HashedId8,
    certificate                     Certificate,
    certificateChain                SequenceOfCertificate,
    certificateDigestWithOtherAlgorithm      CertificateDigestWithOtherAlgorithm,
    ...
}
SequenceOfCertificate ::= SEQUENCE OF Certificate
CertificateDigestWithOtherAlgorithm ::= SEQUENCE  {
    algorithm          PublicKeyAlgorithm,
    digest             HashedId8
}
```

self：自签名，无额外数据。

certificateDigestWithSM3：符合HashedId8结构的8个字节证书摘要信息。

certificate：符合Certificate结构的相关证书信息。

certificateChain：符合Certificate结构的完整证书链信息。链的最后一个元素应包含用于签名消息的证书，倒数第二个元素应包含签署了最后一个证书的CA证书，以此类推。

certificateDigestWithOtherAlgorithm：符合PublicKeyAlgorithm结构公钥算法信息和符合HashedId8结构的8个字节证书摘要信息。

6.5.5 主体信息 SubjectInfo

本项标识了证书的主体信息。该项被定义为SubjectInfo类型，其结构如下：

```
SubjectInfo ::= SEQUENCE  {
    subjectType          SubjectType,
    subjectName          OCTET STRING (SIZE(0..32))
}
```

subjectName中包含了主体信息。subjectName变长向量最大长度为32个字节。

枚举定义主体类型如下：

```
SubjectType::= ENUMERATED {
    enrollmentCredential     (0), //注册证书
    authorizationTicket      (1), //授权证书
    authorizationAuthority   (2), //授权机构
    enrollmentAuthority      (3), //注册机构
    rootCa                   (4), //根认证机构
    crlSigner                (5) //CRL签发者
}
```

当与认证机构通信时,ITS设备应使用SubjectType为enrollmentCredential的SubjectInfo的证书。此类证书禁止用于签发ITS设备注册证书（授权证书）或用于与其他ITS设备认证通信。

当与其他ITS设备通信时,ITS设备应使用SubjectType为authorizationTicket 的SubjectInfo的证书。此类证书禁止用于签发ITS设备授权证书（注册证书）。

授权机构为ITS设备签发授权证书时，SubjectType应当为authorizationAuthority。

认证机构为ITS设备签发注册证书时，SubjectType应当为enrollmentAuthority。

认证机构为其他认证机构签署证书时，SubjectType应当为rootCa。

证书撤销列表的签名者，SubjectType应当为crlSigner。

6.5.6 主体属性 SubjectAttribute

本项标识了证书的主体属性。该项被定义为SubjectAttribute，其结构如下：

```
SubjectAttribute ::= SEQUENCE{
    verificationKey  PublicKey OPTIONAL,
    encryptionKey    PublicKey OPTIONAL,
    assuranceLevel   SubjectAssurance OPTIONAL,
    itsAidList       SequenceOfitsAidList OPTIONAL,
    itsAidSspList    SequenceOfitsAidSspList OPTIONAL,
    ...
}
SubjectAssurance ::= OCTET STRING(SIZE(1))
SequenceOfitsAidList ::= SEQUENCE OF ItsAid
SequenceOfitsAidSspList ::= SEQUENCE OF ItsAidSsp
```

verificationKey/encryptionKey：符合PublicEncryptionKey结构的公钥数据。

assuranceLevel：符合SubjectAssurance结构的主体信任级别。SubjectAssurance：本字段定义ITS设备密钥管理的安全性评估及对应的安全级别。主体信任的规范以及信任水平的编码超出了本文档的范围。默认(没有担保)应当将所有位设置为0。

itsAid：符合IntX类型的一般智能交通应用列表。

```
ItsAid ::= Uint64
```

itsAidSsp：符合ItsAidSsp结构的规定服务权限的智能交通应用列表。

```
ItsAidSsp::= SEQUENCE {
    itsAid                          ItsAid,
    serviceSpecificPermissions      OCTET STRING(SIZE(1..32))
}
```

本结构定义了如何编码规定服务权限的智能交通应用列表。

serviceSpecificPermissions最长为32个字节。

6.5.7 有效性限定 ValidityRestriction

本项标识指定了证书有效性的相关限制。每个证书应包括至少一个具有 time_end 或 time_start_and_end 或time_start_and_duration 类型的 validity_restriction。该项被定义为 ValidityRestriction ，其结构如下：

```
ValidityRestriction ::= CHOICE {
    timeEnd                     Time32,
    timeStartAndEnd             SequenceOfTimeStartAndEnd,
    timestartAndDuration        SequenceOfTimestartAndDuration,
    region                      GeographicRegion,
    ...
}
SequenceOfTimeStartAndEnd ::= SEQUENCE {
    startValidity     Time32,
    endValidity       Time32
}
SequenceOfTimestartAndDuration ::= SEQUENCE {
    startValidity     Time32,
    duration          Duration
}
```

timeEnd：符合Time32结构的证书截止日期。

timeStartAndEnd：符合Time32结构，包含证书有效起始日期以及证书截止日期。

timeStartAndDuration:符合Time32结构的证书有效起始日期以及符合Duration 结构中证书有效时长。

Region：符合GeographicRegion结构的证书有效区域。

6.5.8 签名 Signature

本结构定义了一个容器,该容器用于封装基于公钥密码算法的签名值。其结构如下:

```
Signature ::=CHOICE{
    signature         OCTET STRING (SIZE(32)),
    ...
}
```

6.6 证书撤销列表格式

CRL（证书撤销列表）具有以下结构：

```
Crl ::= SEQUENCE{
    version                    Uint32,
    signerInfo                 SignerInfo,
    unsignedCrl                ToBeSignedCrl,
    signature                  Signature
}
```

证书撤销列表格式示例参见附录B。

version： CRL的版本。在本标准中，此字段设置为1。

signerInfo：标识签名的密钥。该值不能取self。如果包含签名公钥的证书的subjectType为rootCa的话，该值只能取certificateDigestWithSM3。

unsignedCrl：未签名CRL。

Signature：CRL颁发机构签名值。签名基于unsignedCrl字段的内容计算得出。

```
ToBeSignedCrl ::=SEQUENCE{
    type                       CrlType,
    caId                       HashedId8,
    crlSerial                  Uint32,
    startPeriod                Time32,
    issueDate                  Time32,
    nextCrl                    Time32
}
```

caId：发布CRL的CA证书的哈希值的低阶8个字节。

crlSerial：计数器，从0 开始，对于每次颁发CRL时，其值应该增加1。

startPeriod和issueDate指定了此CRL覆盖的时间段。

nextCrl:包含了预计的CRL发布时间。

```
CrlType ::=CHOICE {
    idOnly                     HashedId10,
    idAndExpiry                IdAndDate,
    ...
}
IdAndDate ::=SEQUENCE{
    id                         HashedId10,
    expiry                     Time32
}
```

如果类型是idOnly，条目只列出了证书的ID。

如果类型是idAndExpiry，条目列出了证书的ID以及该证书的有效期。

在这两种情况下，条目应当按HashedId10字段来字典排序。

附 录 A
（资料性附录）
ITS 设备证书格式示例

本部分是一个证书格式的示例，示例数据定义了一个符合Certificate结构的授权证书数据，整个证书结构共159字节。

A.1 消息数据

```
Encoded successfully in 159 bytes:
02811122 33445566 77880108 21212324 25262728 5C801122 33445566 77889900
11223344 55667788 99001122 33445566 77889900 11220101 03000000 00000000
03000000 00000000 04000000 00000000 05010200 00000000 00000108 11121314
15161718 00000000 00000002 08212223 24252627 28810000 00000000 00018031
32333435 36373839 30313233 34353637 38393031 32333435 36373839 303132
```

A.2 数据解析

```
testcert Certificate ::={
    version 2,
    signerInfo  certificateDigestWithSM3 :'1122334455667788'H,
    subjectInfo {
        subjectType authorizationTicket,
        subjectName '2121232425262728'H
    },
    subjectAttributes{
        verificationKey
signKey :'1122334455667788990011223344556677889900112233445566778899001122'H,
        assuranceLevel '01'H,
        itsAidList{
            3,
            4,
            5
        },
        itsAidSspList{
            {
                itsAid 1,
                serviceSpecificPermissions '1112131415161718'H
            },
            {
                itsAid 2,
```

```
                    serviceSpecificPermissions '2122232425262728'H
                }
            }
        },
        validityRestrictions timeStartAndEnd :{
            startValidity 0,
            endValidity   1
        },
        Signature signature:
    '313233343536373839303132333435363738393031323334353637383930313 2'H
    }
```

附 录 B
（资料性附录）
证书撤销列表格式示例

本部分是一个证书撤销列表格式的示例，示例数据定义了一个符合CRL格式的结构，整个证书结构共59字节。

B.1 消息数据

```
Encoded successfully in 81 bytes:
00000001 81112233 44556677 88801112 13141516 17181910 21222324 25262728
00000000 03AC57FC 04E09A20 057ABB32 80313233 34353637 38393031 32333435
36373839 30313233 34353637 38393031 32
```

B.2 数据解析

```
testCRL Crl ::=
{
    version 1,
    signerInfo  certificateDigestWithSM3 :'1122334455667788'H,
    unsignedCrl
    {
        type idOnly : '11121314151617181910'H,
        caId              '2122232425262728'H,
        crlSerial                  0,
        startPeriod            61626364,
        issueDate              81828384,
        nextCrl                91929394
    },
    signature      signature:
'313233343536373839303132333435363738393031323334353637383930313233343536373839303132'H
}
```