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

智能交通 数字证书应用接口规范

Intelligent transport - Certificate application interface

（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 II
1 范围 3
2 规范性引用文件 3
3 术语和定义 3
4 缩略语 4
5 数字证书应用接口 4
6 安全消息语法 5
7 基本元素格式 7
附录A （资料性附录）合作式ITS安全消息示例 12

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。

智能交通 数字证书应用接口

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，规定了安全消息语法中的基本元素格式。

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（包括合作式智能运输系统和车联网等应用）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

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，仅所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 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

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

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。

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。

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。

4 缩略语

以下缩略语适用于本文件。

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

5.1 概述

本规范所定义的证书应用接口包括：获取版本号、消息签名与验证、消息加密与解密、消息信封等。数字证书应用接口处理安全消息，定义的应用数字证书消息的数据结构在第6章说明。

5.2 获取消息版本号

原型： BSTR SOF_GetVersion()
描述： 获取消息的版本号
参数： 无
返回值： 非空 成功
空 失败

5.3 消息签名

原型： BSTR SOF_SignData(BSTR EncodeCert,BSTR InData)
描述： 对消息进行数字签名
参数： EncodeCert[in] 签名者证书

	InData[in]	消息原文
返回值：	非空	安全消息
	空	失败

5.4 验证签名

原型： BOOL SOF_VerifySignedData(BSTR EncodeCert, BSTR SignValue)

描述： 验证消息数字签名

参数：	EncodeCert[in]	签名者证书
	SignValue[in]	安全消息
返回值：	TRUE	成功
	FALSE	失败

5.5 消息加密

原型： BSTR SOF_EncryptData(BSTR EncodeCert,BSTR InData)

描述： 对消息进行数据加密

参数：	EncodeCert [in]	加密用证书
	InData[in]	消息原文
返回值：	非空	安全消息
	空	失败

5.6 消息解密

原型： BSTR SOF_DecryptData(BSTR EncodeCert,BSTR InData)

描述： 对消息进行数据解密

参数：	EncodeCert [in]	解密用证书
	InData[in]	消息原文
返回值：	非空	安全消息
	空	失败

6 安全消息语法

6.1 综述

安全消息语法由多种类型的基本元素构成，基本元素格式在第7章描述，本规范对应的接口处理的数据分为两种类型：

a) 当应用证书类型为机构证书、公务人员证书、社会公众证书、设备证书时，消息数据结构类型遵循 GM/T 0010；

b) 当应用证书类型为 ITS 设备证书时，安全消息数据结构类型遵循本规范。

6.2 合作式 ITS 安全消息语法

6.2.1 安全消息 SecuredMessage

合作式ITS安全消息基本数据结构如下：

```
SecuredMessage  ::= SEQUENCE{
    protocolVersion Uint8,
```

```
    headerFields HeaderField,
    payloadField  Payload,
    trailerFields TrailerField
} SecuredMessage
```

此结构定义了如何编码通用的安全信息:

protocolVersion指定应用的协议版本。为符合当前文档要求，应使用协议版本2。如果标准使用不兼容方法进行了改变，那么protocolVersion应当增加，即语法不兼容会导致老的实现不能解析格式或语义会显著改变。

headerFields是一个包含对安全层感兴趣的多个领域的信息的变长向量。

payloadField 包含消息的有效负载。一个消息不允许多个有效载荷。

trailerFields是一个包含负载后信息的变长向量，例如，需验证信息的真实性和完整性如果消息概要文件中没有另外的定义。

示例参见附录A。

6.2.2 协议版本 ProtocolVersion

本项描述了安全消息的协议版本号。为符合当前文档该值应设为2。

6.2.3 头部字段 HeaderField

头部字段是包含安全消息多项基础信息的变长向量。其结构如下：

```
HeaderField ::= SEQUENCE{
    signerinfo SignerInfo OPTIONAL,
    generationTime Time64 OPTIONAL,
    expiryTime Time64 OPTIONAL,
    generationLocation ThreeDLocation OPTIONAL,
    digests SetOfHashedId3 OPTIONAL,
    itsAid OCTET STRINGOPTIONAL,
    encParams EncryptionParameters OPTIONAL,
    recipients SetOfRecipientInfo OPTIONAL,
    ...
}
SetOfHashedId3 ::= SET OF HashedId3
SetOfRecipientInfo ::= SET OF RecipientInfo
```

signerInfo：给出了SignerInfo结构中包含的消息签名者的信息。如果存在，SignerInfo结构应当为HeaderFields数组中的第一个，除非它被安全配置文件明确覆盖。；

generationTime：消息生成时间，Time64类型的一个时间戳，描述了当安全头内容在签名处理前是固定时的时间点；

expiryTime：代表消息的失效时间；

generationLocation：签名的生成位置；

digests：未识别证书的摘要集合；

itsAid: 代表发送方声明的与有效负载相关联的应用领域；

encParams：符合EncryptionParameters结构的用于加密目的的额外参数。

recipients：消息接收者的集合。给出了变长向量RecipientInfo类型中包含的特定收件人(如使用接收人的公钥加密的数据)的特定信息。

6.2.4 有效负载 Payload

有效负载包含安全消息的具体消息内容，一个消息不允许包含多个有效负载，具体结构如下：

```
Payload ::= CHOICE {
    signedExternal NULL,
    unsecured OCTET STRING,
    signed OCTET STRING,
    encrypted OCTET STRING,
    signedAndEncrypted OCTET STRING,
    ...
}
```

signedExternal：外部签名，无负载数据。

unsecured：未保护信息。

signed：签名信息。

encrypted：加密信息。

signedAndEncrypted：签名加密信息。

6.2.5 尾部字段 TrailerField

```
TrailerField ::= CHOICE {
    signature Signature,
    ...
}
```

signature：符合Signature结构的安全消息签名值。

当payloadField为signedExternal时，待签名信息应在payloadField后，并包含在签名哈希运算内。

当payloadField类型不为“signed ”或“signedAndEncrypted”，则SecuredMessage 的TrailerField字段不应包括签名。

7 基本元素格式

7.1 综述

本标准使用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。本部分定义在合作式智能交通系统数据结构中的基本元素类型，这些元素类型在合作式智能交通系统的安全消息中使用。

7.2 整型

下面的基本类型在数据结构定义中使用：

```
Uint3 ::= INTEGER (0..7)
Uint8 ::= INTEGER (0..255)
Uint16 ::= INTEGER (0..65535)
Uint32 ::= INTEGER (0..4294967295)
Uint64 ::= INTEGER (0..18446744073709551615)
IValue ::= Uint16
```

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
```

7.3 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。

注1:232秒的周期持续约136年，直到2140年。

7.4 64位时间 Time64

```
Time64 ::= Uint64
```

Time64是一个64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微秒数。

7.5 3D位置 ThreeDLocation

```
ThreeDLocation ::= SEQUENCE{
   latitude Latitude,
   longitude Longitude,
   elevation Elevation
}
Latitude ::= NinetyDegreeInt
Longitude ::= OneEightyDegreeInt
Elevation ::= ElevInt
NinetyDegreeInt ::= INTEGER {
    min (-900000000),
    max (900000000),
    unknown (900000001)
} (-900000000..900000001)
KnownLatitude ::= NinetyDegreeInt (min..max)
UnknownLatitude ::= NinetyDegreeInt (unknown)
OneEightyDegreeInt ::= INTEGER {
    min (-1799999999),
    max (1800000000),
    unknown (1800000001)
} (-1799999999..1800000001)
KnownLongitude ::= OneEightyDegreeInt (min..max)
UnknownLongitude ::= OneEightyDegreeInt (unknown)
ElevInt ::= Uint16 -- Range is from -4096 to 61439 in units of one-tenth of a Meter
```

本结构定义了如何指定三维位置。其用来定义证书的有效区域。

Latitude：纬度。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。

Longitude：经度。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。

Elevation：海拔。用分米表示海拔高度，编码如下：

0x0000~0xEFFF:正数的范围从0米 到+6 143.9米。所有高于+6 143.9的数字也由0xEFFF表示。

0xF001~0xFFFF:负数从-409.5米开始,到-0.1米结束。所有低于-409.5的数字也由0xF001表示。

0xF000:未知海拔。

7.6 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。首先计算输入数据的SM3哈希值,取32字节的哈希值的低8个字节。

7.7 3字节哈希值 HashedId3

```
HashedId3 ::= OCTET STRING (SIZE(3))
```

本哈希值用来识别证书等数据。首先计算输入数据的SM3哈希值,取32字节的哈希值的低3个字节。

7.8 公钥算法 PublicKeyAlgorithm

```
PublicKeyAlgorithm ::= ENUMERATED {
    sgdsm3sm2                    (2),
    sgdsm3                       (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。

7.9 对称算法 SymmetricAlgorithm

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

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。

7.10 加密密钥 EncryptKey

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

该结构表示一个加密密钥，它由一个签名密钥和指定的对称加密算法组成。

7.11 公钥 PublicKey

```
PublicKey::= CHOICE{
    signKey OCTET STRING(SIZE(32)),
    encKey EncryptedKey,
    ...
}
```

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。

7.12 加密的对称密钥 SM2EncryptedKey

```
SM2EncryptedKey::= SEQUENCE {
    v  PublicKey,
    c OCTET STRING (SIZE (16)),
    t OCTET STRING (SIZE (16))
}
```

此结构定义了如何传送SM2算法加密的对称密钥。

向量v包含了用于SM2算法加密的发送方的临时密钥。此临时密钥v应只使用一次，每次加密应生成一新的密钥。

向量c包含被加密的对称密钥。

向量t包含身份验证标记。

7.13 加密参数 EncryptionParameters

```
EncryptionParameters ::= CHOICE {
    params (SIZE (12)),
    ...
}
```

该结构包含使用不同对称加密算法的加解密数据所需的基本参数和额外数据。出现aes_128_ccm ，则应该给出一12位八字节的随机数。Tlen 参数应当设置为Tlen = 16字节，同时不需要给出其它相关数据。在其它情况下，数据应当作为一个包含不透明数据的变长向量给出。产生的密文是如何传输的超出了该定义的范围。

7.14 签名者信息 SignerInfo

```
SequenceOfCertificate ::= SEQUENCE OF Certificate

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

}

本项描述了消息签名者的信息。

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。Certificate结构参见标准《智能运输系统 信息安全 数字证书格式》。

certificateChain：符合Certificate结构的完整证书链信息。

certificateDigestWithOtherAlgorithm：定义了其他公钥算法的证书，包括符合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。

7.15 接收者信息 RecipientInfo

```
RecipientInfo ::= SEQUENCE{
    certId HashedId8,
    encKey SM2EncryptedKey
}
```

此结构包含了接收者解密消息的信息。此信息用于分发接收特定的数据。

本标识包含了接收者解密消息的信息。

certId：接收者8字节哈希值的标识。

encKey：符合SM2EncryptedKey结构的加密密钥。

7.16 签名 Signature

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

Signature定义了公钥签名算法的签名值,当前只定义SM2算法的签名。

附　录　A
（资料性附录）
合作式 ITS 安全消息示例

本部分是一个合作式ITS安全消息的示例，示例数据定义了一个符合SecuredMessage结构的数据，有效负载为8字节数据0x3132333435363738，签名数据为：0x1122334455667788 1122334455667788 1122334455667788 1122334455667788，整个消息结构共72字节。

A.1　消息数据

```
02 62 00 81 11 22 33 44 55 66 77 88 00 00 00 00
00 BC 61 4E 00 00 00 00 00 00 27 10 82 08 31 32
33 34 35 36 37 38 80 80 11 22 33 44 55 66 77 88
11 22 33 44 55 66 77 88 11 22 33 44 55 66 77 88
11 22 33 44 55 66 77 88
```

A.2　数据解析

```
SecuredMessage SEQUENCE
  protocolVersion Uint8    2
  headerFields HeaderField
    signerinfo SignerInfo
      certificateDigestWithSM3 HashedId8    0x1122334455667788
    generationTime Time64    12345678
    itsAid ITSAid    10000
  payloadField Payload
    signed    0x3132333435363738
  trailerFields TrailerField
    signature Signature
      signature    0x1122334455667788112233445566778811223344556677881122334455667788
Total encoded length = 72
```