道路交通管控设施数字身份及认证
通用规范

1 范围

本文件规定了道路交通管控设施的数字身份和身份认证要求。

本文件适用于具有车联网车路协同信息交互应用功能的道路交通管控设施。

2 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 2260 中华人民共和国行政区划代码

GB/T 16262.1 信息技术 抽象语法记法一(ASN.1)第1部分:基本记法规范

GB/T 25069 信息安全技术 术语

GB/T 31418 道路交通信号控制系统术语

GM/T 0003 SM2椭圆曲线公钥密码算法

GM/T 0004 SM3密码杂凑算法

GM/T 0009 SM2密码算法使用规范

GM/T 0028 密码模块安全技术要求

ISO/IEC 8825-7 信息技术 抽象语法记法一(ASN.1)编码规则 第7部分 八位字节编码规则(OER)(Information technology - ASN.1 encoding rules:Specification of Octet Encoding Rules(OER))

3 术语和定义

GB/T 25069、GB/T 31418界定的以及下列术语和定义适用于本文件。

3.1

数字身份 digital identity

主体在互联网中的虚拟身份表示,关联了与该主体相关的属性信息,通常由一个账户标识其唯一性。

[来源 GB/T 31504-2015, 3.6]

3.2

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 25069-2022, 3.579]

4 缩略语

ASN.1:抽象语法记法一(Abstract Syntax Nation 1)

CA:证书机构(Certificate Authority)

CRL：证书吊销列表（Certificate Revocation List）
CRACA：证书撤销授权证书机构（Certificate Revocation Authorizing CA）
ID：身份标识（Identity）
SPI：串行外设接口（Serial Peripheral Interface）
SSTL：残余连续终结逻辑（Stub Series Termination Logic）
TTL：晶体管-晶体管逻辑（Transistor-Transistor Logic）

5 数字身份

道路交通管控设施（以下简称“设施”）数字身份应包含设施名称、部署行政区划、设施序号等属性信息，并用编码唯一标识，设施数字身份标识编码应符合附录A的规定。

6 身份认证

6.1 认证方式

设施数字身份认证应采用数字证书认证方式，数字证书应由CA签发。

6.2 数字证书

6.2.1 证书分类

按照数字证书的用途分为：
a) 注册证书：用于应用证书的申请、更新、作废以及注册证书的作废。
b) 应用证书：用于设施的数字身份认证鉴权和信息交互应用。

6.2.2 证书格式

设施数字证书结构应符合附录B的规定，数字证书结构中数据项应符合附录C的规定。

6.2.3 证书载体

应符合以下要求：
a) 载体采用硬件密码模块形式，且符合 GM/T 0028 规定的安全一级要求。
b) 硬件密码模块算法至少包括 SM2、SM3、SM4 国产密码算法。
c) 硬件密码模块存储证书数量：注册证书数量≥2，应用证书数量≥5。
d) 硬件密码模块应用接口符合附录 D 的规定。

6.2.4 证书管理

表1规定了设施数字证书管理流程成要求，证书管理通信接口及数据结构应符合附录F的规定。

表1 证书管理流程要求

序号	证书管理	管理流程要求
1	注册证书申请	应符合附件E.1的规定
2	注册证书作废	应符合附件E.2的规定
3	应用证书申请	应符合附件E.3的规定

表1　证书管理流程要求（续）

序号	证书管理	管理流程要求
4	应用证书更新	应符合附件E.4的规定
5	应用证书作废	应符合附件E.5的规定

6.3　证书确认

设施数字身份认证过程，应对数字证书进行验证确认，至少包括以下验证：

a）　验证 CA 签名：根据当前证书中签发者信息查询签发者证书，并使用签发者证书验证当前证书的数字签名应一致；

b）　验证证书有效期：当前日期应在证书中有效期范围之间；

c）　验证证书状态：如数字证书中 CRL-CA 标识有效，检查证书中指定的证书撤销列表中不应包括证书的证书标识。

附 录 A
（规范性）
数字身份标识编码规则

A.1 编码原则及结构

本文件用 12 位数字分三层表示设施身份标识。

第一层（1～6 位）表示设施部署安装点位所处的行政区。第二层（7～8 位）表示设施的种类。第三层（9～12 位）表示设施在本行政区以及对应设施范围内的唯一编号。

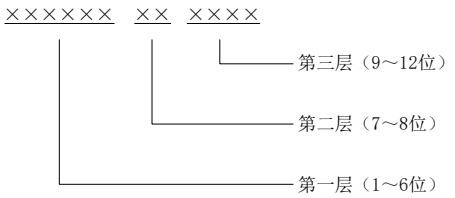

图 A.1 设施身份标识编码

A.2 编码方法

第一层（1～6 位）：设施部署安装点位所处的行政区划编码，包含省、市、县级，6 位数字，取值应符合 GB/T 2260 的规定。

第二层（7～8 位）：设施的索引分类和名称编码，第 7 位标识设施索引分类，第 8 位标识具体设施，代码应符合表 A.1 的规定。

第三层（9～12 位）：设施在本行政区以及对应具体设施范围内的唯一编号，用自然数表示。

表A.1 设施编码

序号	索引分类/代码	设施名称/代码	第二层（7～8位）编码
1	信号控制/01	道路交通信号控制机/01	0101
2		交通控制其他设施/99	0199
3	交通标志/02	可变车道行驶方向标志/01	0201
4		可变限制速度标志/02	0202
5		交通标志其他设施/99	0299
6	边缘计算/03	边缘计算终端/01	0301
7		边缘计算其他设施/99	0399
8	其他交通管控设施/04		0400

附 录 B
（规范性）
数字证书结构

B.1 证书结构

表B.1 数字证书结构

序号	数据项名称/标识		是否必选	说明
1	版本/version		是	证书结构版本，本文件对应版本号为3
2	类型/type		是	证书结构类型，本文件对应类型为显示证书
3	签发者/issure		是	签发此证书的CA证书的8字节哈希值
4	签名数据/tbsigned	证书标识/id	是	证书标识，用设施数字身份标识表示，编码规则按附录A的规定
5		CRL-CA标识/cracaid	是	CRL-CA标识的3字节哈希值
6		CRL序列号/crlSeries	是	CRL序列号
7		有效期/validityPeriod	是	有效期
8		有效地理范围/region	否	有效地理范围（保留暂不使用）
9		保证级别/assuranceLevel	否	保证级别（保留暂不使用）
10		签名权限/appIssuePermissions	是	应用数据签名权限
11		CA证书权限/certIssuePermissions	否	适用于CA证书，描述可签发的证书种类和权限范围（保留暂不使用）
12		注册证书权限/certRequestPermissions	否	适用于注册证书，描述可申请的证书种类、权限范围（保留暂不使用）
13		请求权限/canRequestRollover	否	是否能够请求同等权限的证书（保留暂不使用）
14		加密公钥/encryptionKey	否	加密公钥
15		验证公钥/verifyKeyIndicator	是	验证公钥
16	签名值/signatureValue		是	签名数据的签名值，SM2符合 GM/T 0009要求

附 录 C
（资料性）
数字证书数据结构

C.1 编码规则

数字证书所有字符编码使用 ASN.1 对具体数据结构进行描述，采用八位字节编码规则（Octet Encoding Rules，OER）进行编码。

C.2 数据结构定义

下面的原子类型在数据结构定义中使用：

```
Uint8 ::= INTEGER(0..255)                    --(hex) ff
Uint16 ::= INTEGER(0..65535)                 --(hex) ff ff
Uint32 ::= INTEGER(0..4294967295)            --(hex) ff ff ff ff
```

C.3 证书数据单元

C.3.1 Certificate

```
Certificate ::= CertificateBase(ExplicitCertificate| Reserved)

SequenceOfCertificate ::= SEQUENCE OF Certificate
```

为CertificateBase结构的数据，它指示了数字证书的有效字段组合。

C.3.2 CertificateBase

```
CertificateBase ::= SEQUENCE {
    version         Uint8(3),
    type            CertificateType,
    issuer          IssuerIdentifier,
    tbsigned        ToBeSignedCertificate,
    signatureValue  SignatureValue OPTIONAL
}
```

该数据结构包含以下内容：

——version：证书格式的版本号，此字段应设置为“3”。

——type：指示证书是显式的或其他的。对于显式证书，此字段应设置为 explicit，对于其他证书，此字段应设置为 reserved。本文件对应类型为显示证书。

——issuer：证书的签发方。

——tbsigned：证书的内容。对于显式证书，在生成或校验证书签名时，该字段是哈希函数的输入；对于其他证书类型中的隐式证书，在基于重构值生成或校验公钥时，该字段是哈希函数的输入。该字段的编码细节见 C.3.7 ToBeSignedCertificate。

——signatureValue：包含在 ExplicitCertificate 中。它由 issuer 字段中标识的签名者在 tbsigned 的散列上计算的签名。

C.3.3 CertificateType

```
CertificateType ::= ENUMERATED {
    Explicit,
    reserved
}
```

此枚举类型指示是显示证书或其他类证书。

C.3.4 ExplicitCertificate

```
ExplicitCertificate ::= CertificateBase(WITH COMPONENTS { ...,
    type(explicit),
    toBeSigned(WITH COMPONENTS { ...,
         verifyKeyIndicator(WITH COMPONENTS { verificationKey } )
    }),
    signature PRESENT
})
```

是CertificateBase结构的数据，包含显式证书所需的所有字段。

C.3.5 IssuerIdentifier

```
IssuerIdentifier ::= CHOICE {
    sha256AndDigest         HashedId8,
    self                    HashAlgorithm,
    ...,
    sha384AndDigest         HashedId8,
    sm3AndDigest            HashedId8
}
```

证书的接收方通过这个字段来确定使用哪种密钥材料来验证证书。在本文件中，应用SM3算法。

——该数据结构包含签发证书的 HashedId8，它使用证书的所有字段经哈希散列算法计算得到；

——用于生成证书哈希值以进行验证的哈希算法包括 SM3(在 sm3AndDigest 的情况下)等；

——证书应使用所指示的签发证书的公钥进行验证。

C.3.6 HashedId8

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

该数据结构包含另一个数据结构的截断哈希值。给定数据结构的HashedId8通过计算编码数据结构的散列值、并获取散列输出的低位8个字节来获得当以网络字节顺序表示时，低位8个字节是散列值的最后8个字节。用于计算给定数据结构的HashedId8值的哈希算法取决于上下文。在本文件中，对于包含HashedId8字段的每一个数据结构，均有相应的文字说明如何确定哈希算法。

C.3.7 ToBeSignedCertificate

```
ToBeSignedCertificate ::= SEQUENCE {
    id                      CertificateId,
    cracald                 HashedId3,
    crlSeries               CrlSeries,
    validityPeriod          ValidityPeriod,
    region                  GeographicRegion OPTIONAL,
```

```
    assuranceLevel          SubjectAssurance OPTIONAL,
    appIssuePermissions     SequenceOfAidSsp OPTIONAL,
    certIssuePermissions    SequenceOfAidGroupPermissions OPTIONAL,
    certRequestPermissions  SequenceOfAidGroupPermissions OPTIONAL,
    canRequestRollover      NULL OPTIONAL,
    encryptionKey           PublicEncryptionKey OPTIONAL,
    verifyKeyIndicator      VerificationKeyIndicator,
    ...
}
```

ToBeSignedCertificate结构中的字段具有以下含义。

——id 包含在必要时识别证书持有者的信息。

——cracald 用于识别负责发布证书撤销列表(CRL)的证书撤销授权 CA(CRA)，它的证书可能出现在证书撤销列表(CRL)上。HashedId3 使用全证书哈希算法计算。若不使用 cracald，将该字段设置为全零。

——crlSeries 表示与证书可能出现的特定证书撤销授权 CA(CRACA)相关的 CRL 系列。

——validityPeriod 包含证书的有效期。

——region 表示证书的有效区域，该字段保留暂不使用。

——assuranceLevel 表示证书持有者的保证级别，该字段保留暂不使用。

——appIssuePermissions 表示证书持有者使用此证书签署应用程序数据的权限，该字段保留暂不使用。

——certIssuePermissions 表示证书持有者使用此证书签署其他证书的权限，该字段保留暂不使用。

——certRequestPermissions 表示证书持有者使用此证书签署证书请求的权限，该字段保留暂不使用。

——canRequestRollover 表示该证书可用于签署请求具有相同权限的另一个证书的请求消息，该字段保留暂不使用。

——encryptionKey 包含用于加密的公钥，证书持有者持有相应的私钥。

——verifyKeyIndicator 包含可用于恢复公钥的材料，所恢复的公钥被用于验证被证书签名的数据。

C.3.8 CertificateId

```
CertificateId ::= CHOICE {
    linkageData         LinkageData,
    name                Hostname,
    binaryId            OCTET STRING(SIZE (1..64)),
    none                NULL,
    ...
}
```

此数据结构包含在必要时用于识别证书持有者的信息。

——linkageData 用于识别证书之注销目的，如果该证书出现在链接证书 CRL 中；

——name(名称)用于在非匿名证书的情况下标识证书持有者，它应该是人类可读的；

——binaryId 支持非人类可读的标识符；

——none 表示证书不包含标识符。

C.3.9 HashedId3

```
HashedId3 ::= OCTET STRING(SIZE (3))
SequenceOfHashedId3 ::= SEQUENCE OF HashedId3
```

该数据结构包含另一个数据结构的截断哈希值。给定数据结构的HashedId3通过计算编码数据结构的散列值、并获取散列输出的低位三个字节来获得。当以网络字节顺序表示时，低位三字节是散列值的最后三个字节。用于计算给定数据结构的HashedId3值的哈希算法取决于上下文。在本文件中，对于包含HashedId3字段的每一个数据结构，均有相应的文字说明如何确定哈希算法。

C.3.10 CrlSeries

```
CrlSeries ::= Uint16。
```

这个整形数据结构标识在特定CRACA授权下发布的一系列CRL。若不使用CrlSeries，将该字段设置为零。

C.3.11 ValidityPeriod

```
ValidityPeriod ::= SEQUENCE {
    start           Time32,
    duration        Duration
}
```

该数据类型给出证书的有效期。有效期的开始时间由start指定，结束时间由start+duration决定。

C.3.12 Time32

```
Time32 ::= Uint32
```

该数据类型给出自2004 年1月1日00:00:00 UTC以来的秒数(TAI)。

C.3.13 Duration

```
Duration ::= CHOICE {
    microseconds    Uint16,
    milliseconds    Uint16,
    seconds         Uint16,
    minutes         Uint16,
    hours           Uint16,
    sixtyHours      Uint16,
    years           Uint16
}
```

此数据类型表示证书的有效期。Uint16 值是持续时间，单位由CHOICE选项指示，其中单位“一年”等于31556952秒，这是一年中的平均秒数。

C.3.14 VerificationKeyIndicator

```
VerificationKeyIndicator ::= CHOICE {
    verificationKey         PublicVerificationKey,
    reconstructionValuc     EccP256CurvePoint,
    ...
```

```
}
```

此字段的内容取决于证书是隐式证书还是显式证书:

——verificationKey 出现在显式证书中，它包含用于验证 Certificate(证书)持有者所生成数字签名的公钥;

——reconstructionValue 出现在隐式证书中，它包含重构值，用于恢复国密局隐式证书中指定的公钥。

C.3.15 PublicVerificationKey

```
PublicVerificationKey ::= CHOICE {
    eodsaNistP256           EccP256CurvePoint,
    eodsaBrainpoolP256r1    EccP256CurvePoint,
    ...,
    ecdsaBrainpoolP384r1    EccP384CurvePoint,
    ecdsaNistP384           EccP384CurvePoint,
    ecsigSm2                EccP256CurvePoint
}
```

此数据结构承载公钥，并指示使用该公钥的算法。在本文件中，使用SM2算法。

C.3.16 EccP256CurvePoint

```
EccP256CurvePoint ::= CHOICE {
    x-only              OCTET STRING (SIZE (32)),
    fill                NULL, -- consistency with 1363 / X9.62
    compressed-y-0      OCTET STRING (SIZE (32)),
    compressed-y-1      OCTET STRING (SIZE (32)),
    uncompressedP256 SEQUENCE {
        x               OCTET STRING (SIZE (32)),
        y               OCTET STRING (SIZE (32))
    }
}
```

该数据结构指示在256位素数上定义的Weierstrass形式的椭圆曲线上的点。这包括SM2等算法中定义的椭圆曲线点。该结构中的字段使用IEEEStd1363-2000的椭圆曲线点编码和解码方法来产生的八位字节串。对于CHOICE的所有值，x坐标以网络字节顺序编码成长度为32个八位字节的无符号整数；y坐标的编码取决于该点是仅x，压缩还是未压缩。如果该点是仅x，则省略y；如果该点被压缩，则类型的值取决于y的最低有效位。如果y的最低有效位为0，则类型取值为compressed-y-0，如果y的最低有效位为1，则类型取值compressed-y-1；如果该点未压缩，则y被明确编码为按网络字节顺序的长度为32个八位字节的无符号整数。

C.3.17 PublicEncryptionKey

```
PublicEncryptionKey ::= SEQUENCE {
    supportedSymmAlg    SymmAlgorithm,
    publicKey           BasePublicEncryptionKey
}
```

该数据结构指定公钥和关联的对称加密算法，该算法在加密该公钥时对数据进行批量加密。

C.3.18 SymmAlgorithm

```
SymmAlgorithm ::= ENUMERATED {
    aes128Ccm,
    ..,
    sm4Ccm
}
```

该枚举值指示所支持的对称算法及其操作模式。

C.3.19 BasePublicEncryptionKey

```
BasePublicEncryptionKey ::= CHOICE {
    eciesNistP256           EccP256CurvePoint,
    eciesBrainpoolP256r1    EccP256CurvePoint,
    ...,
    eceneSm2                EccP256CurvePoint
}
```

该数据结构指示特定算法的加密公钥。在本文件中，使用SM2算法。

C.3.20 SignatureValue

```
SignatureValue::= SEQUENCE {
    ecdsaNistP256Signature          EcdsaP256Signature,
    ecdsaBrainpoolP256r1Signature   EcdsaP256Signature,
    ...,
    ecdsaBrainpoolP384r1Signature   EcdsaP384Signature,
    ecdsaNistP384Signature          EcdsaP384Signature,
    sm2Signature                    EcsigP256Signature
}
```

该数据结构表征对应于一个公钥算法的签名。在本文件中，使用SM2算法。

C.3.21 EcsigP256Signature

```
EcsigP256Signature ::= SEQUENCE {
    rSig    OCTET STRING (SIZE (32)),
    sSig    OCTET STRING (SIZE (32))
```

该数据结构表示基于256bit椭圆曲线SM2算法的签名。