www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Translated English of Chinese Standard: GB/T37374-2019

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 03.220.20; 35.240.60

R 07

GB/T 37374-2019

Intelligent Transport - Digital Certificate Application Interface

智能交通 数字证书应用接口规范

Issued on: May 10, 2019 **Implemented on: December 01, 2019**

Issued by: State Administration for Market Regulation;

Standardization Administration of PRC.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Table of Contents

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Intelligent Transport - Digital Certificate Application Interface

1 Scope

This Standard specifies the digital certificate application interface and security message syntax in the intelligent transport system.

This Standard is applicable to the design, research and development, and test of the software and hardware systems related to the digital certificate applications in the intelligent transport system.

2 Normative References

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this document.

GB/T 25069-2010 Information Security Technology – Glossary

GM/T 0010 SM2 Cryptography Message Syntax Specification

3 Terms and Definitions

For the purpose of this document, the terms and definitions given in GB/T 25069-2010 and the following apply.

3.1 Intelligent transport system

In the more improved transport infrastructure, effectively and comprehensively use the advanced science and technology (information technology, computer technology, data communication technology, sensor technology, electronic control technology, automatic control theory, operations research, artificial intelligence, etc.) into the fields of transportation, service control, and vehicle manufacturing; strengthen the contact among the vehicle, road and users; so that form a comprehensive transport system that guarantees safety, increases efficiency, improved environment, and saves energy.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

3.2 Cooperative ITS

An intelligent transport system that realizes intelligent coordination and cooperation between vehicle and infrastructure, between vehicle and vehicle, between vehicle and user through the information interaction of user, vehicle and road.

3.3 Digital certificate

A digital file containing public key owner information, public key, issuer information, expiration date, and some extended information signed by the certification authority.

[GB/T 20518-2006, definition 3.7]

3.4 SM2 algorithm

An elliptic curve cryptographic algorithm with a key length of 256 bits.

3.5 Algorithm identifier

Digital information used to identify algorithmic mechanism.

4 Abbreviations

The following abbreviations are applicable to this document.

ASN.1: Abstract Syntax Notation One

OER: Octet Encoding Rules

ITS: Intelligent Transport System

UTC: Coordinated Universal Time

CBC: Cipher Block Chaining

CFB: Cipher Feedback

OFB: Output Feedback

CCM: Counter with Cipher Block Chaining-Message

5 Digital Certificate Application Interface

5.1 Overview

Digital certification application interface includes message signature and verification,

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Description: verification of message digital signature

Parameters: plain [IN] signature original data buffer area pointer.

plainLen [IN] signature original data length.

signer [IN] encoded byte data buffer area pointer for the signer certificate.

signerLen [IN] signature certificate data length.

pk [IN] verification public key in the signature certificate.

sign [IN] signature value.

Return value: 0 – success; other – verification failure.

5.5 Message asymmetric encryption

The message asymmetric encryption interface is defined as follows:

Prototype: int ITS_AsymEncrypt(unsigned char * plain, int plainLen, int symAlg, PublicKey pk[], EciesEncryptedKey * kek[], CipherText * cipherText)

Description: conduct the data encryption on the message

Parameters: plain [IN] original text to be encrypted.

plainLen [IN] original text length.

symAlg [IN] symmetric encryption algorithm, defined as follows:

```
#define SGD_SM4_ECB     0x401
#define SGD_SM4_CBC     0x402
#define SGD_SM4_CFB     0x404
#define SGD_SM4_OFB     0x408
#define AES_CCM         0x2016
```

pk [IN] encrypted public key from the certificate or signature message.

kek [OUT] the result of encrypting a randomly generated symmetric key using an encrypted public key.

cipherText [OUT] symmetric encryption result.

Return value: 0 – encryption success; other – error.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

The security message syntax structure can be divided into two types:

a) When the application certificate type indicates organization certificate, civil service certificate, social public certificate, device certificate, the security message syntax structure shall follow GM/T 0010;

b) When the application certificate type indicates ITS device certificate, the security message syntax structure shall follow the definition of this Clause.

6.2 Description of basic elements

6.2.1 Encoding rules

The security message syntax consists of several types of basic elements. The following basic element data structure and message syntax are described by using ASN.1; and use OER to encode each information in the signature message and encrypted message.

6.2.2 Basic data type

The basic data type is defined as follows:

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

6.2.3 3-byte hash value

The 3-byte hash value is defined as the HashedId3 type; its structure is as follows:

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

Instruction: this hash value is used to identify the data such as certificates. Firstly, calculate the hash value of the input data; taking the lower 3 bytes of the 32-byte hash value.

6.2.4 8-byte hash value

The 8-byte hash value is defined as the HashedId8 type; its structure is as follows:

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

Instruction: this hash value is used to identify the data such as certificates. Firstly,

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.


```
PublicEncryptionKey ::= SEQUENCE {
    supportedSymmAlg        SymmetricAlgorithm,
    curve                   EccCurve,
    publicKey               ECCPoint
}
```

Instruction: this structure represents a public key for asymmetric encryption calculation and its supported symmetric cryptographic algorithm.

6.2.9 Encrypted symmetric key

The symmetric key for encryption is defined as EciesEncryptedKey type; its structure is as follows:

```
EciesEncryptedKey::= SEQUENCE {
    eccCcurve       EccCurve,
    v       ECCPoint,
    c       OCTET STRING(SIZE(16)),
    t       OCTET STRING(SIZE(32))
}
```

Instruction:

eccCurve indicates the elliptic curve used for asymmetric cryptographic calculation;

Vector v: the temporary key used by the sender for encryption. This temporary key v is used only once; each encryption shall generate new key;

Vector c: contains the encrypted symmetric key;

Vector t: when the public key encryption algorithm is the Chinese cipher algorithm, it corresponds to the M in the Chinese cipher algorithm. When the public key encryption algorithm is the international algorithm, it contains 16-byte authentication token, which is placed in the first 16 bytes; the last 16 bytes are zero.

6.2.10 Signer information

The certificate signer information is defined as SignerInfo type, its structure is as follows:

```
SignerInfo ::= CHOICE {
    self                    NULL,
    certificate             SequenceOfCertificate,
```

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

When not self-signing, it indicates the encoding content of the signer certificate.

6.2.13 32-bit time

The 32-bit time information is defined as Time32 type; its structure is as follows:

```
Time32 ::= Uint32
```

Instruction: Time32 is a 32-bit unsigned integer; in big-endian encoding format; starting from UTC 00:00:00 on January 01, 2004; giving the number of seconds in the international atomic time; the cycle of 2^{32} seconds lasts for 136 years until 2140.

6.2.14 64-bit time

The 64-bit time information is defined as Time64 type; its structure is as follows:

```
Time64 ::= Uint64
```

Instruction: Time64 is a 64-bit unsigned integer; in big-endian encoding format; starting from UTC00:00:00 on January 01, 2004; giving the number of micro-seconds in international atomic time.

6.2.15 3D location information

The 3D location information is defined as ThreeDLocation type; its structure is as follows:

```
ThreeDLocation ::= SEQUENCE {
    latitude        Latitude,
    longitude       Longitude,
    elevation       Elevation
}
Elevation ::= Uint16
```

Instruction: Elevation indicates the height above the sea level; in dm; value range is −4 095(0xF001)dm~61 439(0xEFFF)dm.

6.2.16 Latitude

The latitude information is defined as Latitude type; its structure is as follows:

```
Latitude ::= NinetyDegreeInt
NinetyDegreeInt ::= INTEGER {
    min (−900000000),
```

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------