ICS 03.220.20;35.240.60
CCS R07

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 37376-2024

Transportation - Digital certificate format

交通运输 数字证书格式

Issued on: August 23, 2024 **Implemented on: March 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

1 Scope

GB/T 37376-2024 specifies the digital certificate format for Chinese transportation systems, the credential that lets a vehicle, a roadside unit or a back-office service prove who it is and what it is permitted to assert. Intelligent transport security rests on this format: a certificate has to carry not only an identity and a key but the permissions attached to them, and it has to be small enough to fit in a message broadcast ten times a second and revocable when a unit is compromised. The standard classifies the digital certificates, then defines the certificate format in detail, with normative annexes on the signature calculation process and on the data structures used to encapsulate an ITS certificate revocation list securely, and informative annexes giving a worked example of an ITS certificate and of a CRL. It replaces the 2019 edition and takes effect on 1 March 2025.

This document specifies the requirements for the classification and format of digital certificates in transportation information systems. This document applies to the design, development, testing, application of software and hardware systems related to digital certificates in transportation information systems.

2 Normative references

The contents of the following documents constitute essential clauses of this document through normative references in the text. Among them, for dated references, only the version corresponding to that date applies to this document; for undated references, the

latest version (including all amendments) applies to this document.

GB/T 2659.1 Codes for the representation of names of countries and their subdivisions - Part

3 Terms and definitions

The terms and definitions as defined in GB/T 25069, GB/T 32905, GB/T 32907, GB/T 32918.2, as well as the following terms and definitions, apply to this document.

3.1 Digital certificate A trusted digital document digitally signed by a third-party certificate authority (CA) recognized by the state and with authority, credibility, impartiality. [Source: GB/T 20518-2018, 3.7]

3.2 ITS certificate A digital certificate with a specific format issued to on-board units, roadside units, mobile terminals, operation service providers in intelligent transportation systems.

3.3 SM2 algorithm An elliptic curve public key cryptographic algorithm defined by GB/T 32918. [Source: GB/T 25069-2022, 3.583]

4 Abbreviations

The following abbreviations apply to this document. COER. Canonical Octet Encoding Rules CRACA. Certificate Revocation Authorizing Certificate Authority CRL. Certificate Revocation List ITS. Intelligent Transport System LA. Linkage Authority SPDU. Secured Protocol Data Unit SSP. Service Specific Permissions

5 Classification of digital certificates

The digital certificates issued and managed in the transportation information system include the following 5 categories.

a) Institutional certificates - General format certificates issued to transportation information system institutions;

b) Civil servant certificates - General format certificates issued to end users of transportation information system staff;

c) Social public certificates - General format certificates issued to end users of the public outside the transportation information system;

d) Equipment certificate - General format certificate issued to servers and supporting terminal equipment of transportation information systems;

6 Digital certificate format

6.1 General format Institutional certificates, public servant certificates, social public certificates, equipment certificate formats, certificate revocation lists shall comply with the requirements of GB/T 20518.

6.2.1 Basic elements

6.2.1.1 Encoding rules The data structure defined in this document shall comply with the requirements of GB/T 16262 (all parts). The various information in the digital certificate format shall be encoded using the COER encoding rules specified in ISO/IEC 8825-7.

6.2.1.2 Basic data types The basic data types are defined as follows: The following octet strings are used in the data structure definitions.

6.2.1.3 Application identifier Definition type. Aid 6.2.1.4 3-byte (OCTET) hash value Definition type. HashedId3 6.2.1.5 8-byte (OCTET) hash value Definition type. HashedId

8 Structure. HashedId8..= OCTET STRING (SIZE(8)) SequenceOfHashedId8..= SEQUENCE OF HashedId

8 Description. This data structure contains an 8-byte truncated hash value of another data structure. The HashedId8 of a given data structure is obtained by computing the hash value of the encoded data structure and taking the low-order 8 octets of the hash output. The low-order 8 bytes are the last 8 octets of the hash value, when represented in network byte order. 6.2.1.6 10-byte (OCTET) hash value Type definition. HashedId

10 Structure. HashedId10..= OCTET STRING (SIZE(10)) SequenceOfHashedId10..= SEQUENCE OF HashedId

10 Description. This data structure contains a 10-byte truncated hash value of another data structure. HashedId10 of a given data structure is obtained by computing the hash value of the encoded data structure and taking the low-order 10 octets of the hash output. The low-order 10 bytes are the last 10 octets of the hash value, when represented in network byte order.

6.2.1.7 Hash algorithm Type definition. HashAlgorithm Structure. Description. This data structure represents a hash algorithm. 6.2.1.8 32-bit time Definition type. Time

32 Structure. Time32..= Uint

32 Description. Time32 is a 32-bit unsigned integer, with high-order first encoding format, giving the number of seconds of the International Atomic Time since

08.00.00 Beijing time on January 1, 2004. 6.2.1.9 64-bit time Definition type. Time

64 Structure. Time64..= Uint

64 Description. Time64 is a 64-bit unsigned integer, with high-order first encoding format, giving the number of microseconds of the International Atomic Time since

08.00.00 Beijing time on January 1, 2004.

6.2.2 Certificate

6.2.2.30 Verification key indicator Definition type. VerificationKeyIndicator Structure.

6.3 ITS certificate revocation list

6.3.1 ITS CRL encapsulation format Definition type. SecuredCrl Structure. Description. ITS CRL is defined as a secure encapsulation message, whose content field type is signed data. The signature data payload structure in the signed CRL has no range data extDataHash field; the data field contains ITSSecData, whose content field type is UnsecuredData data and contains signature content. ITSSecData and other ITS CRL security encapsulation related data structures shall comply with the requirements of Appendix C.

6.3.2 ITS CRL content Definition type. CrlContents Structure.

6.3.3 Priority information Definition Type. CrlPriorityInfo Structure.

6.3.6 Revocation certificate link value information Definition type. ToBeSignedLinkageValueCrl Structure.

6.3.7 Revocation batch information Definition type. JMaxGroup Structure. Description. This data structure contains the following information. - jMax is used for the link value-based revocation algorithm. This value applies to all revocation information contained in contents; - contents contains individual link data.

6.3.8 Linkage authority information Definition type. LAGroup Structure.

6.3.9 Total revocation information Definition type. IMaxGroup Structure.

6.3.10 Individual linkage data Definition type. IndividualRevocation Structure. Description. This data structure contains the following information. - linkageSeed1 is used as the LinkageSeed 1 parameter for the revocation algorithm based on the double seed link value; - linkageSeed2 is used as the LinkageSeed 2 parameter for the revocation algorithm based on the double seed link value.

6.3.11 Dual link authority CRL information Definition type. GroupCrlEntry Structure.

6.3.12 Single link authority CRL information Definition type. GroupSingleSeedCrlEntry Structure. Description. This data structure contains the following information.