GM

CRYPTOGRAPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0015-2023

Replacing GM/T 0015-2012

Digital certificate format

数字证书格式

Issued on: December 04, 2023 **Implemented on: June 01, 2024**

Issued by: State Cryptography Administration

Table of Contents

Digital certificate format

1 Scope

This document specifies the basic structure of digital certificates and certificate revocation lists. It describes the content of each data item in digital certificates and certificate revocation lists.

This document applies to the research and development of digital certificate authentication systems, the operation of digital certificate authentication agencies, and security applications based on digital certificates.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 16262.1, *Information technology - Abstract Syntax Notation One(ASN.1) - Part 1: Specification of basic notation*

GB/T 16264.8, *Information technology -- Open systems Interconnection -- The Directory -- Part 8: Public-key and attribute certificate frameworks*

GB/T 17969.1, *Information technology -- Open systems interconnection -- Procedures for the operation of OSI registration authorities -- Part 1: General procedures and top arcs of the International Object Identifier tree*

GB/T 25069, *Information security techniques -- Terminology*

GM/T 0006, *Cryptographic application identifier criterion specification*

GM/T 0009, *SM2 cryptography algorithm application specification*

GM/T 0010, *SM2 cryptography message syntax specification*

GM/Z 4001, *Cryptographic terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB/T 25069 and GM/Z 4001 apply.

5.2.3.5.1 Overview

The certificate validity period is a time period during which the CA guarantees the maintenance of information related to the certificate's status. This item is a sequence of two time values: the start time (notBefore) and the end time (notAfter) of the certificate validity period. Both notBefore and notAfter can be encoded as UTCTime or GeneralizedTime types.

5.2.3.5.2 Coding type requirements

For certificates issued before 2049 (including 2049), the time value shall be encoded using the UTCTime type. For certificates issued after 2050, the time value shall be encoded using the GeneralizedTime type.

5.2.3.5.3 UTCTime

This is a standard ASN.1 type for international applications where local time alone is not sufficient. UTCTime includes a Z (for Zulu, or Greenwich Mean Time) or a time offset.

In this document, UTCTime values shall be expressed using Greenwich Mean Time (Zulu). The year shall use the lowest two digits and include seconds, i.e., the time format shall be YYMMDDHHMMSSZ. The system shall interpret the year field (YY) as follows:

When YY is greater than or equal to 50, the year field shall be interpreted as 19YY. When YY is less than 50, the year shall be interpreted as 20YY.

5.2.3.5.4 GeneralizedTime

This field is a standard ASN.1 type that represents a time with variable precision. The GeneralizedTime field can contain the difference between local time and Greenwich Mean Time.

In this document, GeneralizedTime values shall be expressed in Greenwich Mean Time and shall include seconds, that is, the time format shall be YYYYMMDDHHMMSSZ. The seconds in GeneralizedTime values shall be integers.

5.2.3.6 Subject

This item describes the entity corresponding to the public key in the subject's public key information item. This item may appear in the subject item and/or the subject's optional alternative name extension. If the subject is a CA, then the subject item shall contain a non-empty distinguished name that matches the contents of the issuer item. If the subject's naming information appears only in the subject alternative name extension, then the subject name shall be an empty sequence, and the subject alternative name extension shall be marked critical.

When the Subject field is non-empty, it shall contain a distinguished name. The distinguished name of each subject entity certified by a CA shall be unique. A CA may issue multiple certificates for the same subject entity with the same distinguished name.

The main item structure definition shall comply with the requirements for name types in GB/T 16264.8.

5.2.3.7 Subject Public Key Info

This item contains the certificate public key and the corresponding public key algorithm. The public key algorithm is represented by the AlgorithmIdentifier structure.

When the public key algorithm is SM2, the AlgorithmIdentifier structure definition shall comply with GM/T 0010. When the public key algorithm is RSA, the AlgorithmIdentifier structure definition is given in RFC8017.

5.2.3.8 issuerUniqueID

This field is used to address the reuse of issuer names. The issuer unique identifier varies for different issuers. In v1, CAs that comply with this document shall not include this field in certificates issued by them. However, when parsing certificates containing this extension, applications shall correctly parse the value of this field.

5.2.3.9 subjectUniqueID

This field is used to address subject name reuse. The subject unique identifier is different for different subjects. In version 1, CAs that comply with this document shall not include this field in certificates issued by them. However, when parsing certificates containing this extension, applications shall correctly parse the value of this field.

5.2.3.10 extensions

This item is a sequence of one or more certificate extensions (SEQUENCE). Its content and data structure are described in 5.2.4.

5.2.4 Certificate extension fields and their data structure

5.2.4.1 Certificate extensions

Certificate extensions include standard extensions and specialized extensions. An extension consists of three parts: the extension type, the extension's criticality, and the extension's value. The extension's criticality can be defined as critical or non-critical, indicating whether a certificate user can ignore the extension. If a certificate application system cannot recognize a critical extension, it shall reject the certificate. If it cannot recognize a non-critical extension, it can ignore the information in that extension.

This section defines some standard extensions. It shall be noted that in actual application, if critical extensions are used, it may make the certificate unusable in some

common applications.

Each extension consists of an object identifier (OID) and an ASN.1 structure. When an extension appears in a certificate, the OID appears as the extnID element, and its corresponding ASN.1 encoding structure is the 8-bit string extnValue. A particular extension shall appear only once in a certificate. An extension contains a Boolean value indicating the criticality of the extension; the default value is FALSE, indicating non-criticality.

A CA shall support the Authority key identifier, subject key identifier, basic constraints, key usage, and certificate policies extensions. Other extensions are optional. If the subject field in a CA-issued certificate contains an empty sequence, the CA shall support the subject alternative name extension. A CA may support extensions beyond those defined in this document, but if such extensions are defined as critical, this may hinder interoperability.

Applications shall recognize at least the following extensions: key usage, certificate policy, subject alternative name, basic constraints, name constraints, policy constraints, and extended key usage. Additionally, the authority key identifier, subject key identifier, and policy mapping extensions shall be supported.

5.2.4.2 Standard extensions

5.2.4.2.1 Overview

This section defines standard certificate extensions for digital certificates. The OIDs defined in 16 extensions, from 5.2.4.2.2 to 5.2.4.2.17, shall comply with GB/T 16264.8. These OIDs are members of id-ce and are defined as follows:

```
id-ce      OBJECT IDENTIFIER ::=  { joint-iso-ccitt(2) ds(5) 29 }
```

The OIDs of the six extension definitions from 5.2.4.2.18 to 5.2.4.2.23 shall comply with GM/T 0006.

5.2.4.2.2 authorityKeyIdentifier

This extension provides a way to identify the public key corresponding to the certificate's signing private key. This extension is used when the issuer has multiple signing keys, either due to coexistence or changes in the key. The authority key identifier can be based on the subject key identifier in the CA certificate or on the issuer's name and serial number.

All certificates issued by a CA must include the keyIdentifier field in the issuing authority key identifier extension to facilitate certificate chaining. When a CA issues its public key in a self-signed certificate, the CA key identifier field may be omitted. In this case, the subject and CA key identifiers are identical.

This field can be used as either a certificate extension or a CRL extension. It identifies

c) keyEncipherment: Encrypt keys or other security information, such as for key transport;

d) dataEncipherment: Encrypt user data, but does not include keys or other security information specified in c) above;

e) keyAgreement: Used as a public key agreement key;

f) keyCertSign: Verify the CA signature of a certificate;

g) cRLSign: Verify the CA signature of a CRL;

h) encipherOnly: When this bit is used with the keyAgreement bit set, the public key agreement key is used only to encrypt data (the meaning of this bit used with other key usage bits set is undefined);

i) decipherOnly: When this bit is used with the keyAgreement bit set, the public key agreement key is used only to decrypt data (the meaning of this bit used with other key usage bits set is undefined).

keyCertSign is used only in CA certificates. If KeyUsage is set to keyCertSign and the basic constraints extension is present in the same certificate, then the value of the cA field of the basicConstraints extension shall be set to TRUE. A CA may also use other key usage bits defined in the keyUsag [Translator's note: keyUsage?] extension, for example, to provide authentication and integrity for online management transactions.

If the keyAgreement bit is not set, the meaning of the encipherOnly bit is undefined. If the encipherOnly bit is set, and the keyAgreement bit is also set, the subject public key can be used only to encrypt data while performing key agreement.

If the keyAgreement bit is not set, the meaning of the decipherOnly bit is undefined. If the decipherOnly bit is set, and the keyAgreement bit is also set, the subject public key can be used only to decrypt data while performing key agreement.

All CA certificates shall include this extension and shall include the usage of keyCertSign. This extension may be defined as either critical or non-critical, at the option of the certificate issuer.

If this extension is marked critical, then the certificate shall only be used for purposes for which the corresponding key usage bit is set to "1".

If this extension is marked non-critical, it indicates the intended use or uses of this key and can be used to find the correct key/certificate for an entity with multiple keys/certificates. It is a recommendation and does not imply that the use of this key is limited to the specified use. A bit set to "0" indicates that this key is not intended for that use. If all bits are "0", it indicates that this key is intended for a use other than the listed uses.

```
id-ce-nameConstraints OBJECT IDENTIFIER::={ id-ce 30 }
NameConstraintsSyntax::=SEQUENCE{
    permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
    excludedSubtrees        [1]     GeneralSubtrees OPTIONAL}
GeneralSubtrees::=SEQUENCE SIZE (1..MAX) OF GeneralSubtree
GeneralSubtree::=SEQUENCE{
    base                    GeneralName,
    minimum                 [0]     BaseDistance DEFAULT 0,
    maximum                 [1]     BaseDistance OPTIONAL}
BaseDistance::=INTEGER(0..MAX)
```

If the permittedSubtrees and excludedSubtrees fields are present, they each specify one or more named subtrees, each defined by the name of the subtree's root or, optionally, by the name of any node within its subtrees. A subtree scope is a region bounded by an upper bound and/or a lower bound. If permittedSubtrees is present, only certificates issued by the subject CA and subordinate CAs in the certification path that have a subject name identical to the one specified in the permittedSubtrees field are acceptable. If excludedSubtrees is present, any certificates issued by the subject CA or subsequent CAs in the certification path that have a subject name identical to the one specified in excludedSubtrees are unacceptable. If both permittedSubtrees and excluded Subtrees are present and the namespaces overlap, the exclusion declaration in excluded Subtrees takes precedence.

The naming formats defined by the GeneralName field shall use name forms with a well-defined hierarchical structure for these fields. The Directory Name format meets this requirement. Subtrees named using these naming formats correspond to DIT subtrees. Applications shall not check and recognize all possible naming formats. If this extension is marked as critical, and the naming format used for the base item is not recognized by the certificate usage, the certificate shall be processed as if it had encountered an unrecognized critical extension. If this extension is marked as non-critical, and the naming format used for the base item is not recognized by the certificate usage, the subtree specification may be ignored. When a certificate subject has multiple names with the same name form (including the name in the certificate subject item, if non-"0", in the case of the directory Name format), all of these names shall be verified.

Restrictions may be placed on the subject name or subject alternative name. Restrictions apply only when the specified name format is present. If no such name is present in the certificate, the certificate is acceptable. When testing the certificate subject name for conformance to naming format restrictions, even entries marked as non-critical in the extension shall be processed.

The minimum field specifies the upper boundary of this region within the subtree. All names whose last named form is above the specified level are not included in this region. A minimum value of "0" corresponds to the base, i.e., the top node of the subtree. For example, if minimum is set to "1", the naming subtree does not include the root node but only the nodes below it.

5.3.3.3 issuer

This field identifies the entity that signs and issues the CRL. It shall contain a non-empty distinguished name (DN -- distinguished name). This field is defined as a Name type.

The encoding rules for issuer are the same as those in 5.2.3.4.

5.3.3.4 thisUpdate

This field specifies the date the CRL was issued, encoded using UTCTime or GeneralizedTime.

For CRLs issued before 2049 (including 2049), the time value shall be encoded using the UTCTime type. For CRLs issued after 2050, the time value shall be encoded using the GeneralizedTime type.

The encoding rules for UTCTime are the same as those in 5.2.3.5.3.

The encoding rules for GeneralizedTime are the same as those in 5.2.3.5.4.

5.3.3.5 nextUpdate

This field specifies the time when the next CRL will be published. The next CRL can be issued before this time, but not after. Use UTC or GeneralizedTime encoding.

The CRL issuer shall include a nextUpdate entry in the CRL it issues.

For CRLs issued before 2049 (including 2049), the time shall be encoded as the UTCTime type. For CRLs issued after 2050, the time shall be encoded as the GeneralizedTime type.

The encoding rules for UTCTime are the same as those in 5.2.3.5.3.

The encoding rules for GeneralizedTime are the same as those in 5.2.3.5.4.

5.3.3.6 Revoked Certificates

This item indicates the serial number, revocation time and certificate revocation list entry extension of the revoked certificate.

If there is no revoked certificate, this item does not exist. Otherwise, this item shall contain the serial number of the revoked certificate and the date of revocation.

5.3.3.7 crlExtensions

This field can only appear in a v2 CRL. It consists of a sequence of one or more CRL extensions.

crlExtensions is described in 5.3.4.

5.3.4 CRL extensions

5.3.4.1 authorityKeyIdentifier

This extension provides a way to identify the public key corresponding to the private key that signed the CRL. This extension is used when the issuer has multiple keys or has multiple signing keys due to changes.

5.3.4.2 issuerAltName

This extension contains one or more alternative names for use by the CRL issuer.

This extension shall be non-critical.

5.3.4.3 crlNumber

For a CRL issuer, the values represented by this field in a series of CRLs issued by the issuer may form a monotonically increasing sequence. This field allows users to easily determine when a particular CRL supersedes another. The certificate revocation list number shall support distinguishing between full and incremental CRLs. This field is a non-critical CRL extension.

If a CRL issuer generates a delta CRL in addition to a full CRL for a specific scope, the full and delta CRLs shall use the same number. If the full and delta CRLs are issued at the same time, they shall use the same certificate revocation list number and provide the same revocation information.

If a CRL issuer generates two CRLs (possibly two full CRLs, or two incremental CRLs, or one full CRL and one incremental CRL) at different times within a specific range, that is, the thisUpdate fields of the two CRLs are different, then the two CRLs cannot use the same certificate revocation list number.

CRL verifiers shall be able to process CRL numbers that are 20 bytes long. CRL issuers shall use CRL numbers that are no longer than 20 bytes.

```
id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }
  CRLNumber ::= INTEGER (0..MAX)
```

5.3.4.4 delta CRLIndicator

This field identifies a CRL as a delta CRL. A delta CRL contains certificate revocation information added since the last issuance, rather than including all revocation information in a full CRL. This field shall be marked as critical.

This extension contains a value of type BaseCRLNumber. The certificate revocation

Annex C

(normative)

Certificate contents

C.1 General

This appendix defines a series of certificate content tables. Each table defines the certificate content for a specific type of certificate or certificate revocation list. And in the issuer attribute, there are optional features widely supported in the PKI system. In practical applications, certificates and certificate revocation lists may include non-critical extension information in local applications, but PKI clients may not need to process these additional information. In addition, key extensions that are not listed in the worksheet shall not be used in the content of PKI certificates or certificate revocation lists.

The certificate contents include the following contents.

a) The self-signed CA certificate content table, also known as the root certificate content worksheet, defines the mandatory and optional content for self-signed certificates. When a trust root is confirmed, the CA in the PKI system issues a self-signed certificate.

b) The content table of the second level CA certificate defines the mandatory and optional content of the second level CA certificate.

c) The content table of the terminal entity signature certificate defines the mandatory and optional content of the entity signature certificate issued by CA. Its object is a terminal entity. Its private key is used for signing. Its public key is used to verify the signature. The key pair of this certificate is generated on the client side during issuance and is private to the user. Its private key shall not be able to be exported from the terminal medium.

d) The terminal entity encryption certificate content table defines the mandatory and optional content of entity encryption certificates issued by CAs in the PKI system. Its public key is used to encrypt data. The private key is used to decrypt data. The key is distributed by the Key Management Center (KM). Its lifecycle is controlled by the key management center. During the validity period of the certificate, if the medium is damaged, it can be restored through the normal process through the CA center.

e) The certificate revocation list content table defines the mandatory and optional content of the certificate revocation list published by the certificate revocation list issuer.

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

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