ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0092—2020

基于SM2算法的证书申请语法规范

Specification of certificate request syntax based on SM2 cryptographic algorithm

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京信安世纪科技股份有限公司、格尔软件股份有限公司、北京数字认证股份有限公司、长春吉大正元信息技术股份有限公司、兴唐通信科技有限公司、卫士通信息产业股份有限公司、国家信息安全工程技术研究中心、山东得安信息技术有限公司、北京创原天地科技有限公司。

本文件主要起草人：汪宗斌、刘婷、郑强、傅大鹏、赵丽丽、王妮娜、赵闪、罗俊、张旭、周淑静、张庆勇、焦靖伟、史晓峰、马洪富。

引　言

本文件的内容参照证书请求语法规范(RFC2986 PKCS#10),按照我国相关密码政策和规范,结合我国实际应用需求及产品生产厂商的实践经验,定义了基于SM2算法的证书申请和证书申请信息语法格式,增添了证书申请信息的扩展属性和证书响应格式。

证书申请,由证书申请信息、数字签名算法和对证书申请信息的数字签名三部分组成。其中,证书申请信息又包括可区分的主体名称、主体公钥信息、一组可选属性集。

证书申请发送到证书认证机构之后,证书认证机构将该申请转换为数字证书。

基于SM2算法的证书申请语法规范

1 范围

本文件定义了使用SM2密码算法的证书申请语法、证书申请信息的扩展属性和证书响应格式。

本文件适用于数字证书认证系统的研制，数字证书应用系统使用SM2密码算法进行证书申请操作时，对证书申请语法的标准化封装。

2 规范性引用文件

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 31503—2015 信息安全技术 电子文档加密与签名消息语法

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 33560—2017 信息安全技术 密码应用标识规范

GB/T 35275—2017 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

证书 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进行数字签名的一个可信的数字化文件。

3.2

签名 signature

由GB/T 32905定义的一种算法。由一个应用程序通过密码算法用私钥运算所产生的值，具有完整性，消息鉴别和/或签名者鉴别的特性。

3.3

属性 attributes

由对象的属性和一个相关属性值组成的集合。

4 缩略语

下列缩略语适用于本文件。

ASN.1：抽象语法标记(Abstract Syntax Notation One)

BER：基本编码规则(Basic Encoding Rule)

CA:证书认证机构(Certificate Authority)

DER:对 ASN.1 的唯一编码规则(Distinguished Encoding Rules),DER 是 BER 的一个子集。

OID:对象标识符(Object Identity)

5 OID 定义

本文件对 3 个对象 certificationRequestInfo、certificationRequest、challengePassword 的标识符进行了定义,详见表 1。

表 1 对象标识符

对象标识符 OID	对象标识符定义
1.2.156.10197.6.1.4.1.10	基于 SM2 算法的证书申请语法规范
1.2.156.10197.6.1.4.1.10.1	证书申请信息类型 certificationRequestInfo
1.2.156.10197.6.1.4.1.10.2	证书申请类型 certificationRequest
1.2.156.10197.6.1.4.1.10.3	挑战口令类型 challengePassword

6 证书申请语法

6.1 CertificationRequestInfo 结构

证书申请信息应符合 ASN.1 的类型 CertificationRequestInfo:(下面仅列出部分 ASN.1,完整的 ASN.1 定义按附录 A 执行)

```
CertificationRequestInfo ::= SEQUENCE {
version         INTEGER {v1(0)},
subject         Name,
subjectPKInfo   SubjectPublicKeyInfo,
attributes      [0] Attributes{{ CRIAttributes }}
}
```

其中,

```
Attributes { ATTRIBUTE:IOSet } ::= SET OF Attribute{{ IOSet }}
Attribute           { ATTRIBUTE:IOSet } ::= SEQUENCE {
type                    ATTRIBUTE.&id({IOSet}),
values      SET SIZE(1..MAX) OF ATTRIBUTE.&Type({IOSet}{@type})
}
```

CertificationRequestInfo 类型组成见表 2。

表 2 CertificationRequestInfo 数据类型

字段名称	数据类型	含义
version	INTEGER	语法的版本号
subject	Name	证书申请主体名称
subjectPublicKeyInfo	SubjectPublicKeyInfo	主体的公钥信息,其数据类型按 GB/T 35275—2017 的 13.2
attributes	Attributes	主体的扩展属性集

6.2 CertificationRequest 结构

证书申请应符合 ASN.1 的类型 CertificationRequest：(下面仅列出部分 ASN.1，完整的 ASN.1 定义按附录 A 执行)

```
CertificationRequest ::= SEQUENCE {
    certificationRequestInfo        CertificationRequestInfo,
    signatureAlgorithm              AlgorithmIdentifier,
    signature                       BIT STRING
}
```

其中，

```
AlgorithmIdentifier::= SEQUENCE {
    Algorithm       OBJECT IDENTIFIER,
    parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

这里的 AlgorithmIdentifier 用来标识签名算法，其中 OBJECT IDENTIFIER 标识具体的算法，可选参数的内容完全依赖于所标识的算法。本文件的签名算法为基于 SM2 算法和 SM3 算法的签名，无参数。其 OID 按 GB/T 33560—2017。

CertificationRequest 类型组成见表 3。

表 3 CertificationRequest 数据类型

字段名称	数据类型	含义
certificateRequestInfo	CertificateRequestInfo	证书申请信息，被签名的信息
signatureAlgorithm	SignatureAlgorithm	主体的私钥对证书申请信息签名的算法

主体发送证书申请一般发生在公私钥对生成之后，或变更主体甄别名称之后。在证书申请时，对证书申请信息进行签名是为了防止主体使用他方的公钥进行证书申请。签名过程有以下两个步骤组成：

a) CertificationRequestInfo 的组成部分被 DER 编码，产生字节串；

b) a)的结果用证书申请主体的私钥和特定的签名算法签名，产生一个位串，也就是签名。

7 证书申请信息的扩展属性

ChallengePassword 属性类型指定了一个口令，使用该口令，主体可以进行证书申请或者证书作废。挑战口令属性应有唯一的属性值。

一个挑战口令应符合 ASN.1 类型的 ChallengePassword：

```
ChallengePassword ::= PrintableString
```

8 证书响应格式

证书响应包括：签名证书、已加密的加密证书私钥和加密证书。具体格式如下：(下面仅列出部分 ASN.1，完整的 ASN.1 定义按附录 A 执行)

```
CSRResponse :: =SEQUENCE{
    signCertificate                 CertificateSet,
```

```
    encryptedPrivateKey          [0] SM2EnvelopedKey OPTIONAL,
    encryptCertificate           [1] CertificateSet OPTIONAL
}
```

CSRResponse 类型组成见表 4。

表 4　CSRResponse 数据类型

字段名称	数据类型	含义
signCertificate	CertificateSet	签名证书。证书链的集合，其数据类型定义按 GB/T 31503—2015 的 12.2.3
encryptedPrivateKey	SM2EnvelopedKey	SM2 私钥的密文。SM2EnvelopedKey 数据类型定义按 GB/T 35276—2017 的 7.4
encryptCertificate	CertificateSet	加密证书。证书链的集合，其数据类型定义按 GB/T 31503—2015 的 12.2.3

附 录 A
（规范性）
ASN.1 语法

本附录将本文件中的 ASN.1 语法在这里作为 ASN.1 结构定义给出。

```
CSR {iso(1) member-body(2) cn(156) cstc(10197) pkcs(6) bc(1) sm(4) pkcs-10(10) modules(1) csr(1)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- EXPORTS All --
-- All types and values defined in this module are exported for use in other ASN.1 modules. IMPORTS informationFramework,
authenticationFramework FROM UsefulDefinitions joint-iso-itu-t(2) ds(5) module(1) usefulDefinitions(0) 3} ATTRIBUTE,
Name FROM InformationFramework informationFramework
ALGORITHM FROM AuthenticationFramework authenticationFramework;
-- Certificate requests
CertificationRequestInfo ::= SEQUENCE {
    version          INTEGER {v1(0)},
    subject          Name,
    subjectPKInfo    SubjectPublicKeyInfo,
    attributes       [0] Attributes{{ CRIAttributes }}
}
SubjectPublicKeyInfo  ::= SEQUENCE {
    Algorithm      AlgorithmIdentifier,
    subjectPublicKey      BIT STRING
}
Attributes { ATTRIBUTE:IOSet } ::= SET OF Attribute{{ IOSet }}
CRIAttributes  ATTRIBUTE  ::= { ... -- add any locally defined attributes here -- }
Attribute { ATTRIBUTE:IOSet } ::= SEQUENCE {
    type                        ATTRIBUTE.&id({IOSet}),
    values SET SIZE(1..MAX) OF ATTRIBUTE.&Type({IOSet}{@type})
}
CertificationRequest ::= SEQUENCE {
    certificationRequestInfoCertificationRequestInfo,
    signatureAlgorithm   AlgorithmIdentifier,
    signature    BIT STRING
}
AlgorithmIdentifier {ALGORITHM:IOSet } ::= SEQUENCE {
    algorithm               ALGORITHM.&id({IOSet}),
    parameters   ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}
```

```
SignatureAlgorithms ALGORITHM ::= { ... -- add any locally defined algorithms here -- }
ChallengePassword ::= PrintableString
CSRResponse :: =SEQUENCE{
    signCertificate                CertificateSet,
    encryptedPrivateKey[0] EncryptedData OPTIONAL,
    encryptCertificate [1] CertificateSet OPTIONAL
}
END
```

参 考 文 献

[1] GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法
[2] RFC2985 PKCS #9: Selected Object Classes and Attribute Types Version 2.0
[3] RFC2986 PKCS #10: Certification Request Syntax Standard Version 1.7

中华人民共和国密码
行业标准
基于SM2算法的证书申请语法规范
GM/T 0092—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.75 字数 23千字
2021年4月第一版 2021年4月第一次印刷
*
书号:155066·2-35939 定价 18.00元

GM/T 0092-2020

码上扫一扫 正版服务到