GM

CRYPTOGRAPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

CCS L 80

GM/T 0092-2020

Specification of certificate request syntax based on SM2 cryptographic algorithm

基于 SM2 算法的证书申请语法规范

Issued on: December 28, 2020 **Implemented on: July 01, 2021**

Issued by: National Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2020 “Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents”.

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of Cryptographic Industry Standardization Technical Committee.

The drafting organizations of this Standard: Beijing Xin'an Century Technology Co., Ltd., Geer Software Co., Ltd., Beijing Digital Certification Co., Ltd., Changchun Jitai Zhengyuan Information Technology Co., Ltd., Xingtang Communication Technology Co., Ltd., Weishitong Information Industry Co., Ltd., National Information Security Engineering Technology Research Center, Shandong De’an Information Technology Co., Ltd., Beijing Chuangyuan Tiandi Technology Co., Ltd.

Main drafters of this Standard: Wang Zongbin, Liu Ting, Zheng Qiang, Fu Dapeng, Zhao Lili, Wang Nina, Zhao Shan, Luo Jun, Zhang Xu, Zhou Shujing, Zhang Qingyong, Jiao Jingwei, Shi Xiaofeng, Ma Hongfu.

Specification of certificate request syntax based on SM2 cryptographic algorithm

1 Scope

This document defines the certificate request syntax that uses SM2 cryptographic algorithm, the extended attributes of the certificate request information, and the certificate response format.

This document is applicable to the development of digital certificate authentication system. When the digital certificate application system uses SM2 cryptographic algorithm for certificate request operations, it encapsulates the standardization of the certificate request syntax.

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 31503-2015, *Information security technology - Encryption and signature message syntax for electronic document*

GB/T 32905, *Information security technology SM3 cryptographic hash algorithm*

GB/T 33560-2017, *Information security technology - Cryptographic application identifier criterion specification*

GB/T 35275-2017, *Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification*

GB/T 35276-2017, *Information security technology - SM2 cryptography algorithm usage specification*

GM/Z 4001, *Cryptographic terms*

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GM/Z

4001 as well as the followings apply.

3.1 certificate

a credible digital document that is digitally signed by an authoritative, credible and impartial third-party certificate certification body recognized by the state

3.2 signature

an algorithm defined by GB/T 32905; it is a value generated by an application program that uses a cryptographic algorithm to calculate with a private key; with the characteristics of integrity, message authentication and/or signer authentication

3.3 attributes

a collection of object attributes and a related attribute value

4 Abbreviations

The following abbreviations apply to this document.

ASN.1: Abstract Syntax Notation One

BER: Basic Encoding Rule

CA: Certificate Authority

DER: Distinguished Encoding Rules for ASN.1; DER is a subset of BER

OID: Object Identity

5 Definition of OID

This document defines the identifiers of the three objects certificationRequestInfo, certificationRequest, and challengePassword, see Table 1.

Where,

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

AlgorithmIdentifier here is used to identify the signature algorithm. OBJECTIDENTIFIER identifies the specific algorithm. The content of the optional parameters completely depends on the identified algorithm. The signature algorithm of this document is a signature based on SM2 algorithm and SM3 algorithm, without parameters. Its OID is in accordance with GB/T 33560-2017.

The type composition of CertificationRequest is shown in Table 3.

The subject sending a certificate application generally occurs after the public and private key pair is generated, or after the subject's distinguished name is changed. When applying for a certificate, the purpose of signing the certificate request information is to prevent the subject from using the other party's public key for certificate request. The signing process consists of the following two steps:

a) The components of CertificationRequestInfo are encoded by DER to generate a byte string;

b) The result of a) is signed with the private key of the subject of the certificate request and a specific signature algorithm to generate a bit string, that is, a signature.

7 Extended attributes of certificate request information

ChallengePassword attribute type specifies a password. Using this password, the subject can apply for a certificate or revoke the certificate.

The challenge password attribute shall have a unique attribute value.

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

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