

ICS 35.040
CCS L 80

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0089-2020

Simple certificate enrollment protocol specification

简单证书注册协议规范

(English Translation)

Issued on: December 28, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Foreword	1
Scope	2
Normative references	3
Terms and definitions	4
Abbreviations	5
Overview	6
RA	7
Client certification	8
Enrollment certification	9
CA/RA certificate distribution	10
Certificate enrollment	11
CRL query	12
Certificate revocation	13
Overview	14
SCEP message structure	15
Signing time (signingTime)	16
Overview	17
Certificate enrollment	18
Overview	19
Transaction success	20
Simplified SignedData data type	21
Request message format	22
Request message format	23
Response message format	24
Request message format	25
Response message format	26
Request message format	27
Response message format	28
Request message format	29
Request message format	30
Request message	31
Request message	32

Request message	33
Response message	34
Request message	35
Request message	36
Foreword	37
Request message	38
Request message	39
Request message	40
Response message	41
Request message	42
Request message	43

Foreword

This document is drafted in accordance with 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 document may be the subject of patent rights. The issuing authority of this document shall not be held responsible for identifying any or all such patent rights.

This document was proposed by and shall be under the jurisdiction of Cryptography Standardization Technical Committee.

Drafting organizations of this document. Changchun Jilin University Zhengyuan Information Technologies Co., Ltd., Beijing Infosec Technologies Co., Ltd., Koal Software Co., Ltd., Westone Information Industry INC., Feitian Technologies Co., Ltd., Beijing Certificate Authority Co., Ltd., Xingtang Telecommunications Technology Co., Ltd., Shanghai Electronic Certification Authority Co., Ltd., Beijing WatchSmart Technologies Co., Ltd., Beijing HuaDa ZhiBao Electronic System Co., Ltd., Beijing Creative Century Technology Co., Ltd., Shandong Dean Information Technology Co., Ltd.

Main drafters of this document. Zhao Lili, Zhang Qingyong, Zheng Qiang, Zhang Liting, Luo Jun, Zhu Pengfei, Fu Dapeng, Wang Nina, Han Wei, Wang Xuelin, Zhang Yuan, Chen Baoru, Wang Xiaochen, Ma Hongfu.

1 Scope

This document defines a simple protocol for certificate enrollment using the SM2 algorithm.

This document is applicable to guiding the development of a digital certificate authentication system that provides automatic certificate enrollment, as well as the use of SM2 algorithm

for automatic enrollment of device certificates.

2 Normative references

The contents of the following documents, through normative references in this text, constitute indispensable provisions of this document. Among them, for dated references, only the edition corresponding to that date applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 20518-2018 Information security technology - Public key infrastructure - Digital certificate format
GB/T 32918 (all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves
GB/T 35275-2017 Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification
GM/T 0092 Specification of certificate request syntax based on SM2 cryptographic algorithm
GM/Z 4001 Cryptology Terminology

3 Terms and definitions

The terms and definitions defined by GM/Z 4001 and the following ones apply to this document.

Client

The device which applies for certificate service.

Note: The client is also called the requester.

Server

The entities which provide certificate services, including CA and RA.

Digital envelope

A data structure which contains a ciphertext encrypted with a symmetric key and the symmetric key encrypted with a public key.

4 Abbreviations

The following abbreviations apply to this document.

CA. Certification Authority CDP. CRL Distribution Point CGI. Common Gateway Interface

5.1.1 Overview

SCEP entities include client and server. The server is composed of CA and RA.

SCEP describes the protocol process and format of the client's enrollment and certification with the server. The entity relationship of SCEP is shown in Figure 1.

5.1.4 RA

RA is a kind of SCEP server. It performs certification and authorization checks on SCEP clients. At the same time, the certification request is forwarded to the CA. The name of the RA shall not appear in the issuer field of the generated certificate.

5.2 Client certification

In order to encrypt and sign data according to the syntax format of GB/T 35275, the client shall have an available local certificate.

5.3 Enrollment certification

The server can set a policy, to automatically or manually enroll and authenticate the client's request.

5.4 CA/RA certificate distribution

If the client has not obtained a CA/RA certificate before, starting any PKI operation, it shall apply for a CA/RA certificate.

5.5 Certificate enrollment

The client creates a certificate request according to GM/T 0092 to start the certificate enrollment transaction; and sends it to CA/RA after encapsulating it according to GB/T 35275.

5.7 CRL query

SCEP clients can obtain CRL through one of the following two methods.

5.8 Certificate revocation

SCEP does not specify the method for requesting certificate revocation.

6.1 Overview

SCEP messages with confidentiality requirements adopt a two-layer structure, see GB/T 35275. By simultaneously applying digital envelope and digital signature, the end-to-end transaction information integrity and confidentiality of the information part of the SCEP message are protected.

6.2.1 SCEP message structure

The basic structure of all secure SCEP message objects is the SCEP message.