ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0089—2020

简单证书注册协议规范

Simple certificate enrollment protocol specification

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：长春吉大正元信息技术股份有限公司、北京信安世纪科技股份有限公司、格尔软件股份有限公司、成都卫士通信息产业股份有限公司、飞天诚信科技股份有限公司、北京数字认证股份有限公司、兴唐通信科技有限公司、上海市数字证书认证中心有限公司、北京握奇智能科技有限公司、北京华大智宝电子系统有限公司、北京创原天地科技有限公司、山东得安信息技术有限公司。

本文件主要起草人：赵丽丽、张庆勇、郑强、张立廷、罗俊、朱鹏飞、傅大鹏、王妮娜、韩玮、汪雪林、张渊、陈保儒、王晓晨、马洪富。

引　言

简单证书注册协议是一种证书管理的简单协议，主要用于客户端(用户)与服务端(CA/RA)之间的证书自动注册。它结合了 PKCS#7 和 PKCS#10，保证了证书注册的安全可靠。而且在大规模的设备证书自动注册中简化了对请求者身份鉴别的工作，令设备证书的注册变得更为简单。

本文件的内容参考了 IETF 的《Simple Certificate Enrollment Protocol》Internet-Draft 稿，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，制定了适应我国证书体系和密码算法的简单证书注册协议。

简单证书注册协议规范

1 范围

本文件定义了使用SM2算法进行证书注册的简单协议。

本文件适用于指导研制提供证书自动注册的数字证书认证系统，以及使用SM2算法进行设备证书的自动注册。

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 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

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

GM/T 0092 基于SM2算法的证书申请语法规范

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

客户端 client

申请证书服务的设备。

注：客户端也称请求端。

3.2

服务端 server

提供证书服务的实体，包含CA和RA。

3.3

数字信封 digital envelope

一种数据结构，包含用对称密钥加密的密文和用公钥加密的该对称密钥。

3.4

设备证书 device certificate

数字证书的一种，由CA签名的包含设备的基本信息、设备公钥信息及其他补充信息等的一种数据结构。

3.5

SM2算法 SM2 algorithm

由GB/T 32918(所有部分)定义的一种算法。