ICS 35.040
CCS L 80

GM

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。

4 缩略语

下列缩略语适用于本文件。

CA:证书认证机构(Certification Authority)

CDP:证书撤销列表分发点(CRL Distribution Point)

CGI:公共网关接口(Common Gateway Interface)

CRL:证书撤销列表(Certificate Revocation List)

LDAP:轻量级目录访问协议(Lightweight Directory Access Protocol)

PKI:公钥基础设施(Public Key Infrastructure)

RA:证书注册机构(Registration Authority)

SCEP:简单证书注册协议(Simple Certificate Enrollment Protocol)

5 SCEP 功能

5.1 SCEP 实体

5.1.1 概述

SCEP 实体包含客户端和服务端。服务端由 CA 和 RA 组成。SCEP 描述客户端向服务端注册认证的协议流程及格式。SCEP 实体关系见图 1。

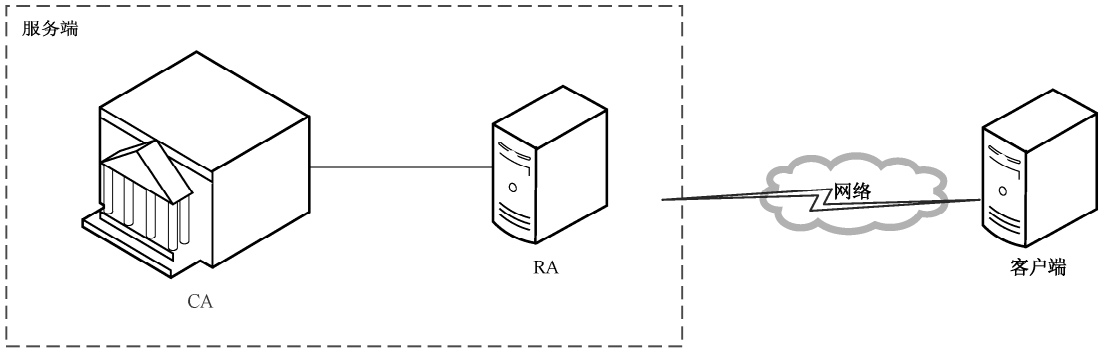

图 1 SCEP 实体关系图

客户端在注册认证的过程中,如果以前没有获取 CA/RA 证书,则应在任何 PKI 操作启动之前申请获取 CA/RA 证书,得到 CA/RA 证书后进行证书注册流程,在进行注册认证后,客户端可以向 CA 进行证书查询和 CRL 查询,在 CA 证书更新时及时获取下一个 CA 证书。

5.1.2 客户端

客户端开始一个 PKI 事务之前,应至少有一张能够对 SCEP 消息进行签名的证书。

客户端应配置如下的信息。

a) CA 或 RA 的 IP 地址或域名。

b) CA 或 RA 的 HTTP 脚本路径。

c) CA 的相关辨识信息,可以是 CA 证书的杂凑值。辨识信息或来自用户,或在协议交互时通过人工授权传递给终端用户。

客户端应采取可靠措施,对这些信息的完整性进行保护。

客户端可维护适用于多个 CA 的多个独立配置,这些配置并不影响协议操作。

5.1.3 CA

CA 是签发客户端证书的实体，CA 的名字应出现在生成证书的签发者字段中。

在任何 PKI 操作发生之前，CA 应获得一个符合 GB/T 20518—2018 配置的 CA 证书，这可以是上级 CA 签发的 CA 证书。

客户端应通过 7.1.1 的获取 CA 证书请求消息得到 CA 证书，并将获取 CA 证书响应消息所得到的 CA 证书通过证书杂凑值进行认证。

CA 应在线回应证书查询请求或通过 LDAP 提供证书查询结果。

CA 可实施任何策略并应用这些策略认证或拒绝客户端的请求。如果服务端已经为客户端签发过证书，且该证书在当前仍然有效，服务端可返回之前为客户端创建的证书。

如果客户端在轮询一个挂起事务后进入超时状态，它应通过向服务端发送与证书注册事务名称、密钥和事务 ID 相同的请求，来进行重新同步。CA 应返回证书注册事务的状态，包括已发放的证书。CA 不应创建新事务，除非已注册的证书被撤销或超过有效期。

5.1.4 RA

RA 是一种 SCEP 服务端，它对 SCEP 客户端进行认证和授权检查，同时将认证请求转发给 CA。在生成证书的签发者字段中应不出现 RA 的名称。

RA 在通过 7.1.2 的获取 CA 证书响应消息返回证书时应同时返回 RA 证书和 CA 证书，此响应中包括一个 RA 证书，说明该客户端正在通过一个 RA 向 CA 提出证书相关的请求，客户端在后续的安全通信中应将指定该 RA 作为服务端通信。

为了进行认证服务，RA 应将请求传递给 CA 服务端进行处理，CA 与 RA 之间的通信协议在本文件中不做规定。

5.2 客户端认证

为了按照 GB/T 35275 语法格式对数据进行加密和签名，客户端应有一个可用的本地证书。

a) 如果客户端已经有一个 SCEP 服务端签发的证书，且服务端支持更新，应使用该证书。

b) 如果客户端没有 SCEP 服务端 CA 签发的证书，但具有来自其他 CA 的证书，则应使用其他 CA 签发的证书。在新 CA 上的策略设置将决定是否认可其他 CA 认证结果、是否为客户端服务。

c) 如果客户端没有服务端 CA 签发的证书及来自备用 CA 的证书，应使用本地生成的基于 SM2 算法的自签名证书替代。自签名证书应使用与 GM/T 0092 要求相同的主体名称。

在证书注册期间，客户端在遵循 GB/T 35275 进行签名时，应使用选定的证书。客户端发送请求后，服务器端生成响应，在服务器端对响应进行加密时，需使用此签名证书的公钥。

5.3 注册认证

服务端可设置策略，对客户端的请求进行自动注册认证或手动注册认证。

在自动注册认证模式下，服务端应实现适当的逻辑，对客户端进行签名的证书进行自动认证，并使用由认可的其他 PKI 层次体系中 CA 颁发的现有客户端凭证进行自动注册。

在手动注册认证模式下，客户端消息一直处于挂起状态，直到 CA 操作员对该消息进行确认或者拒绝。

客户端生成 GM/T 0092 的申请消息的杂凑值，并使用其他可靠的带外传输方式发送给 CA 操作员。CA 操作员应将此杂凑值与在 SCEP 交互时收到消息后在本地生成的杂凑值进行比较，验证其完整性。

5.4 CA/RA 证书分发

客户端如果以前没有获取 CA/RA 证书，则应在任何 PKI 操作启动之前申请获取 CA/RA 证书。

在客户端获取 CA 证书之后，应使用杂凑算法对接收到的 CA 证书（及可能含有的 RA 证书）计算杂凑值，如果客户端没有到信任锚的证书路径，则通过将证书杂凑值与本地配置的、带外方式得到的信息进行比较，来对 CA 证书进行身份认证。

由于客户端和 CA/RA 之间尚未交换公钥，因此无法按照 GB/T 35275 的语法格式来保护这些消息，而数据将在明文中传输。

如果 RA 正在使用中，则按 GB/T 35275 中的 SignedData 类型格式返回一个数字信封，信封中或包含 RA 和 CA 证书，或只有 CA 证书本身。传输协议应指明返回的是哪一个。

在客户端获取 CA 证书之后，应使用杂凑算法对接收到的 CA 证书（及可能含有的 RA 证书）计算杂凑值，如果客户端没有到信任锚的证书路径，则通过将证书杂凑值与本地配置的、带外方式得到的信息进行比较，来对 CA 证书进行身份认证。

由于从客户端到 CA/RA 之间传递查询可能耗费很长时间，而 RA 证书可能随时更改，因此建议客户端不要存储 RA 证书，而应在每次操作之前检索 CA/RA 证书。

5.5 证书注册

客户端按照 GM/T 0092 创建一个证书请求来启动证书注册事务，并将其按照 GB/T 35275 封装后发送到 CA/RA。

如采用自动注册认证模式，CA/RA 根据策略返回请求响应消息 CertRep，状态设置为 SUCCESS 或 FAILURE。消息类型定义见 6.2.2.3。

如采用手动注册认证模式，CA/RA 返回的 CertRep 消息的状态设置为 PENDING，则客户端应通过定期向 CA/RA 发送获取证书轮询 GetCertInitial 来进入轮询模式，直到 CA/RA 操作员完成手动身份验证，批准或拒绝该请求。

如果进入轮询模式，客户端应发送单个证书请求 PKCSReq 消息，后跟 0 个或多个 GetCertInitial 消息。CA/RA 将发送 0 个或多个 CertRep 消息，状态设置为 PENDING，CA/RA 最后发送一个 CertRep 消息，状态为 SUCCESS 或 FAILURE。

在证书注册期间，客户端状态转换在图 2 中表示。

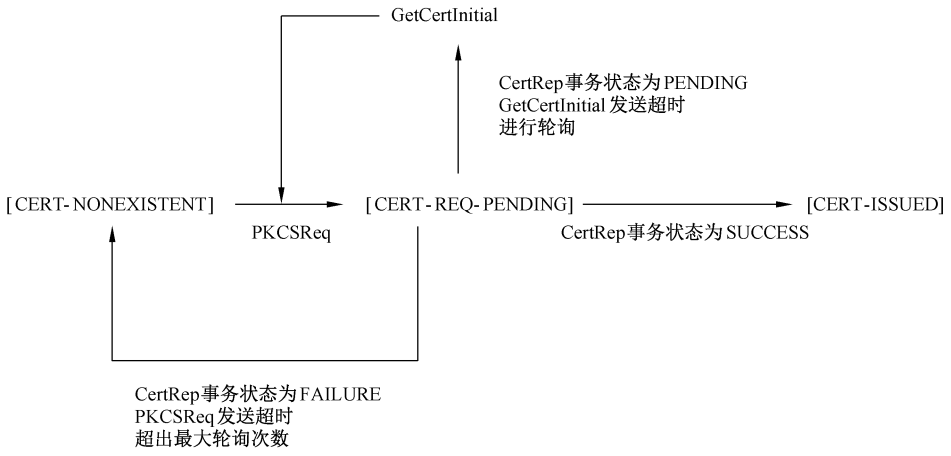

图 2 状态转换图

证书注册从状态 CERT-NONEXISTANT 开始。

发送 PKCSReq 消息会将状态更改为 CERT-REQ-PENDING。如果没有响应，或无法发送，状态恢复到 CERT-NONEXISTANT。

接收到事务状态 pkiStatus 为 SUCCESS 的 CertRep 消息，将会把状态更改为 CERT-ISSUED。

接收到事务状态 pkiStatus 为 FAILURE 的 CertRep 消息，将会把状态更改为 CERT-NONEXISTANT。

如果服务端发送的 CertRep 消息的事务状态 pkiStatus 为 PENDING，则客户端将通过定期向服务端发送 GetCertInitial 消息来进行轮询，直到接收到状态设置为 SUCCESS 或 FAILURE 的 CertRep 消息，或者已超过最大轮询次数。

如果超过了最大轮询数，或者在 CERT-REQ-PENDING 状态下收到了 pkiStatus 设置为 FAILURE 的 CertRep 消息，则最终客户端将进入 CERT-NONEXISTANT 状态，并且 SCEP 客户端最终可以开启另一个注册请求。应注意的是，只要客户端不更改其主体名称或密钥，就会在新事务中使用相同的事务 ID。这一点很重要，因为基于此事务 ID，证书认证机构可以将其识别为已有的事务，而不是当作新事务来处理。

自动模式下的成功事务流程见图 3。

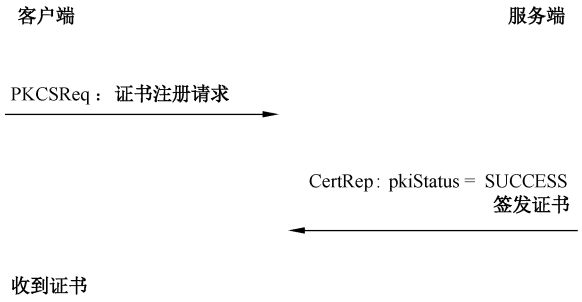

图 3　自动模式事务

手动模式下成功的事务见图 4。

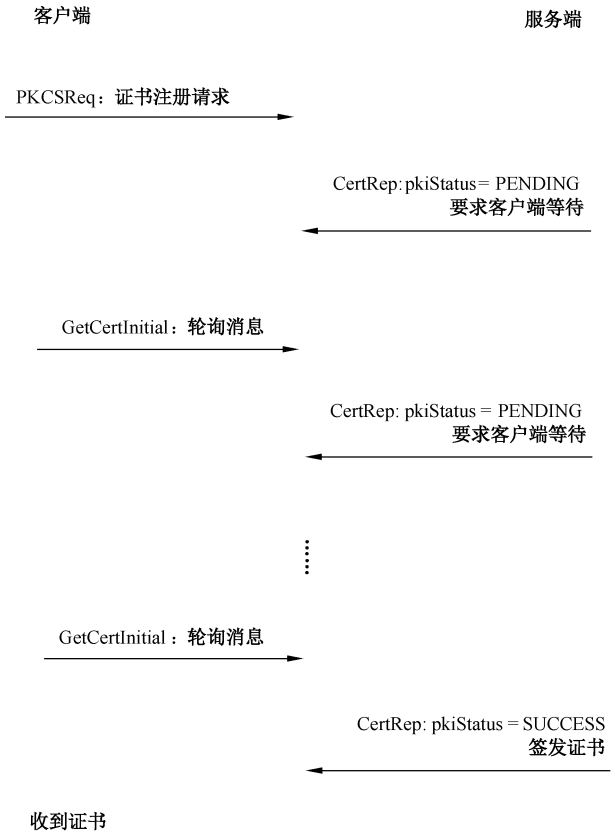

图 4　手动模式事务

5.6 证书查询

为客户端定义了证书查询消息，以便从 CA 检索自己的证书副本。它允许不在本地存储证书的客户端在需要时获取副本。此功能不用于提供通用证书目录服务。

要从证书认证机构查询证书，客户端将发送由证书签发者名称和序列号组成的请求。假定客户端已在以前的注册事务中将签发证书的签发者名称和序列号保存下来。查询证书的事务由一个 GetCert 消息和一个 CertRep 消息组成，见图 5。

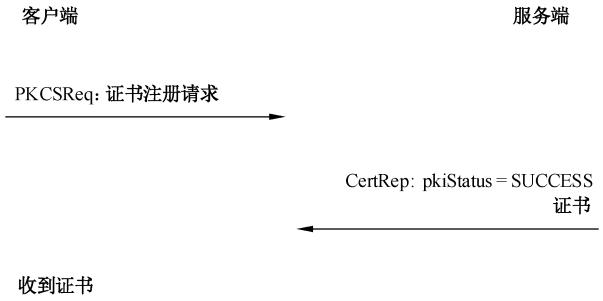

图 5 GetCert 事务

5.7 CRL 查询

SCEP 客户端可通过以下两种方法之一获得 CRL：

a) 如果 CA 支持 CDP，则应通过 CDP 中指定的机制查询 CRL；

b) 如果 CA 不支持 CDP，则通过创建一个由 GetCRL 消息构成的 CRL 查询，该消息由一个待检索 CRL 范围内的证书的签发者名称和序列号组成。

服务端宜使用 CDP 方法。

消息以与其他 SCEP 请求相同的方式发送到 SCEP 服务端：要检索 CRL 的事务由一个 GetCRL 消息和一个 CertRep 消息组成，其中只包含 CRL，见图 6。

在收到此消息后，SCEP 服务端可以使用 IssuerAndSerial 信息返回适当的 CRL。

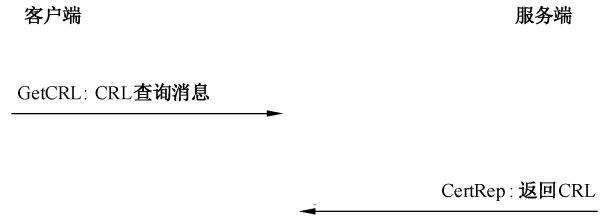

图 6 GetCRL 事务

5.8 证书撤销

SCEP 不指定请求证书撤销的方法。

6 SCEP 安全消息对象

6.1 概述

有机密性需求的 SCEP 消息采用两层结构，见 GB/T 35275。通过同时应用数字信封和数字签名，

对 SCEP 消息的端到端事务信息完整性和信息部分的机密性进行保护。

外层的 ContentType 字段应是数字签名 SignedData 结构，也称为 pkiMessage；内层的 ContentInfo 字段应为 EnvelopedData 结构，也称为 pkcsPKIEnvelope。SCEP 消息携带的数据 messageData 封装在 pkcsPKIEnvelope 里，其数据格式由 pkiMessage 中的 messageType 属性定义。

如果没有传输 messageData，则整个 pkcsPKIEnvelop 应忽略。例如，状态为 FAILURE 和 PENDING 的 CertRep 消息没有签名信息。

6.2 SCEP 消息

6.2.1 SCEP 消息结构

所有安全 SCEP 消息对象的基本结构是 SCEP 消息，该结构由 GB/T 35275 中的 SignedData 类型组成，如 GB/T 35275—2017 中 8.1 所定义。存在如下的限制：

如果出现了被签名的内容(CertRep 消息为 SUCCESS 状态)，该内容应是 pkcsPKIEnvelope 结构，并应匹配 messageType 属性。

6.2.2 被签名的事务属性

6.2.2.1 概述

按照 GB/T 35275—2017 的 8.2，SignedData 的 SignerInfo 需要承载一系列认证属性(authenticatedAttributes)。所有消息都应包括 transactionID、messageType 、senderNonce 及其他任何 GB/T 35275—2017 中 8.2 需要的属性。如果是响应消息，则应包括 pkiStatus、recipientNonce 属性，见表 1。

表 1 认证属性

属性	编码	注释
transactionID	PrintableString	杂凑值
messageType	PrintableString	十进制数
pkiStatus	PrintableString	十进制数
failInfo	PrintableString	十进制数
senderNonce	OCTET STRING	—
recipientNonce	OCTET STRING	—

6.2.2.2 事务标识(transactionID)

一个 PKI 操作就是一次包括客户端和服务端之间消息交换的事务。事务标识是事务开始时客户端产生的字符串。客户端应为事务标识产生唯一的字符串，编码为可打印字符串，在一次给定注册过程的所有 PKI 消息中使用。

事务标识应是注册请求所注册公钥值的杂凑值。这样可以允许 SCEP 客户端为任意给定密钥对自动产生相同的事务标识，以便于后续的轮询能够匹配之前的事务。当使用本文件定义的证书和证书撤销列表查询消息时，需要使用事务标识来确保客户端将响应消息与之前的请求消息相匹配。当使用 LDAP(轻量级目录服务协议)来查询证书和证书撤销列表时，具体的行为过程由 LDAP 确定。对于非注册消息(例如 GetCert 和 GetCRL)，事务标识应是对客户端唯一的数字。

6.2.2.3 消息类型(messageType)

消息类型属性确定事务所执行操作的类型。这个属性应包含在所有的 PKI 消息中。如下消息类型已被定义:

PKCSReq(19)	GM/T 0092 证书请求
CertRep(3)	请求响应
GetCertInitial(20)	证书轮询
GetCert(21)	证书查询
GetCRL(22)	CRL 查询

未定义的消息类型作为错误处理。

6.2.2.4 事务状态(pkiStatus)

所有的响应消息应包括事务状态信息,定义为 pkiStatus:

SUCCESS(0)	批准
FAILURE(2)	拒绝,并提供 6.2.2.5 中定义的 failInfo 属性
PENDING(3)	待处理

未定义的消息类型作为错误处理。

6.2.2.5 失败信息(failInfo)

失败信息属性应包括下列失败原因:

badAlg (0)	不能识别或未被支持的算法标识
badMessageCheck (1)	完整性校验失败
badRequest (2)	事务未被允许或支持
badTime (3)	签名时间属性和系统时间不够接近
badCertId (4)	没有识别出可以匹配所提供标准的证书

未定义的消息类型作为错误处理。

6.2.2.6 发送者随机数和接受者随机数(senderNonce 和 recipientNonce)

发送者随机数 senderNonce 和接受者随机数 recipientNonce 是每个事务产生的 16 字节随机数。用来抗重放攻击。

客户端应在发送给服务端的 PKI 消息中包含发送者随机数。

服务端应将发送者随机数复制到 recipientNonce,客户端应校验 recipientNonce。

6.2.2.7 签名时间(signingTime)

签名时间属性指定签名者执行签名过程的时间,该属性可选。其定义可参考 PKCS#9。

6.2.3 SCEP 数字信封

SCEP 消息的信息部分包含在 EnvelopedData 类型中,如 GB/T 35275—2017 第 9 章所述,有以下限制:

a) encryptedContent 应是被传送的 SCEP 消息,应和 pkiMessage 里的 mesaageType 认证属性匹配;

b) GB/T 35275 使用消息接收方的公钥加密传输密钥。

6.3 SCEP 消息类型

6.3.1 概述

SCEP 消息的类型应是在 messageType 认证属性中指定。以下章条定义了有效的消息类型、对应的消息数据格式，还有这个类型强制性的认证属性。

6.3.2 证书注册

这个类型的 MessageData 域包含一个 GM/T 0092 证书请求，证书注册可包含 GM/T 0092 中定义的任意域，同时应要包含至少以下几项：

——主体标识名；

——主体公钥；

——ChallengePassword 属性，ChallengePassword 可能被用来认证注册请求自身。

除有效 GB/T 35275 所需要的 authenticatedAttributes 以外，pkiMessage 应还要包含以下几个属性：

——事务标识属性 transactionID；

——消息类型属性 messageType，设置为 PKCSReq；

——发送者随机数属性 senderNonce。

正如 6.2.3 所描述的，这种消息类型的 pkcsPKIEnvelope 属性由接收者的公钥保护。

6.3.3 证书注册响应

6.3.3.1 概述

这种类型的 messageData 属性包含一个如 6.4 所示的简化的 SignedData，回复所需要的确切内容依赖于这个消息回复的请求类型，在表 1 和第 4 章有具体描述。

除有效 GB/T 35275 所需要的 authenticatedAttributes 以外，pkiMessage 应还要包含以下几个属性：

——事务标识属性 transactionID：从请求消息中复制；

——消息类型属性 messageType：设置为 CertRep；

——发送者随机数属性 senderNonce；

——接受者随机数属性 recipientNonce：从申请消息的发送者随机数属性 senderNonce 复制得到；

——事务状态 pkiStatus。

正如 6.1.2 所描述的，这种消息类型的 pkcsPKIEnvelope 属性由接收者的公钥保护。例如，如果一个自签名证书用来发送请求，那么这个自签名证书的公钥就要用来加密 SUCCESS 回应的 pkcsPKIEnvelope 属性的内容加密密钥。

SignedData 数据中 contentInfo 字段存储了 SM2 加密证书私钥数据，其数据格式遵循 GB/T 35275 中第 10 章 signedAndEnvelopedData。SignedData 的 certificates 字段存放着为客户端签发的 SM2 证书，第一个是签名证书，第二个是加密证书。

6.3.3.2 事务成功

当事务状态被设置为 SUCCESS，这个消息的 messageData 包含一个如 6.4 定义的简化的数字信封，其内容取决于证书注册请求，如表 2 所示。

表 2　CertRep 类型

请求类型	响应内容
PKCSReq	回复应至少包含签名数据的证书域中向请求者颁发的证书。回复可以包含附加证书，但颁发的证书应处在列表中的首位。回复一定不包含 CRL。所有返回的证书应符合 GB/T 20518—2018
GetCertInitial	和 PKCSReq 一样
GetCert	回复应至少包含签名数据的证书域中请求的证书。回复可以包含附加证书，但请求的证书应处在列表中的首位。回复一定不包含 CRL。所有返回的证书应符合 GB/T 20518—2018
GetCRL	回复应包含签名数据的 crls 域中的 CRL。回复一定不包含证书。符合 GB/T 20518—2018 要求的 CRL 才能被认为是有效的

6.3.3.3　事务失败

当事务状态被设置为 FAILURE，响应应包含一个 failInfo 属性，来描述失败的原因。pkcsPKIEnvelope 应省略。

6.3.3.4　事务待处理

当事务状态被设置为 PENDING。pkcsPKIEnvelope 应省略。

6.3.4　证书轮询

这种类型的 messageData 属性包含一个证书签发者与主体 IssuerAndSubject。签发者被设置为证书认证机构的 issuerName，主体被设置为请求证书时使用的 SubjectName。

除有效 GB/T 35275 所需要的 authenticatedAttributes 以外，pkiMessage 应还要包含以下几个属性：

——和 PKCSReq 消息中相同的事务标识属性 transactionID；

——消息类型属性 messageType，设置为 GetCertInitial；

——一个 senderNonce 属性。

IssuerAndSubject 类型的定义如下：

```
IssuerAndSubject::=SEQUENCE{
    issuerName,
    subjectName
}
```

6.3.5　证书查询

这种类型的 messageData 包含一个 IssuerAndSerialNumber，IssuerAndSerialNumber 是在 GB/T 35275 中定义的，唯一确定了请求的证书。

除有效 GB/T 35275 所需要的 authenticatedAttributes 以外，pkiMessage 应还要包含以下几个属性：

——事务标识属性 transactionID；

——消息类型属性 messageType，设置为 GetCert；

——发送者随机数属性 senderNonce。

6.3.6 CRL 查询

这种类型的 messageData 包含一个 IssuerAndSerialNumber，其定义在 GB/T 35275—2017 的 6.7，包含需要确认的证书发布者姓名和序列号。

除有效 GB/T 35275 所需要的 authenticatedAttributes 以外，pkiMessage 应还要包含以下几个属性：

——事务标识属性 TransactionID；

——消息类型属性 messageType，设置为 GetCRL；

——发送者随机数属性 senderNonce。

6.4 简化的 SignedData 数据类型

简化的 SignedData 数据类型是指 GB/T 35275 中签名数据类型 SignedData 的简化，其没有签名者，只是为了传送证书和证书吊销列表。

在携带证书时，证书将包含在 SignedData 的 certificates 字段中。在携带 CRL 时，CRL 将包含在 SignedData 的 crls 字段中。

7 SCEP 事务

7.1 获取 CA 证书

7.1.1 请求消息格式

为了得到 CA 证书，客户端发送一个 GetCACert 消息到服务端。此消息中没有相关数据。

7.1.2 响应消息格式

响应消息格式取决于服务端是否具有 RA 证书或只有一个 CA 证书，服务端应明确指定它发送的是何种响应。

所有返回的证书格式应符合 GB/T 20518—2018。

如果服务端就是 CA 证书认证机构，并且没有任何 RA 证书，那么响应由一个 CA 证书组成。

如果服务端具有 RA 证书，则响应消息就是一个简化的 SignedData 数据类型，其中只包含 CA 证书和 RA 证书。

7.2 证书注册

7.2.1 请求消息格式

PKCSReq 消息用于证书注册申请。

先决条件：客户端和 CA 认证机构都已经完成了初始化过程。客户端已经配置了 CA/RA 证书。

后置条件：客户端收到证书，请求可以被拒绝，或者请求待处理。待处理的响应可能表明需要人工认证。

7.2.2 响应消息格式

响应消息应是一个服务端返回的 CertRep 消息，分为成功(SUCCESS)、失败(FAILURE)或待处理(PENDING)三种状态。

如果请求被授予，返回一个事务状态为 SUCCESS 的 CertRep 消息，响应消息应包含签发的证书。

如果请求被拒绝，则返回一个事务状态为 FAILURE 的 CertRep 消息，响应消息应包含 failInfo 属性。

如果 CA 配置为对客户端的验证为人工方式，则返回一个事务状态为 PENDING 的 CertRep 消息，CA 也可能因为其他原因返回 PENDING。

7.3 证书轮询

7.3.1 请求消息格式

由事务状态为 PENDING 的 CertRep 触发，客户端将通过定期发送 GetCertInitial 状态查询请求到服务端，从而进入轮询状态，直到请求被授予并且证书被发回，或者请求被拒绝，或者超过配置的轮询时间限制（或最大轮询次数）。

由于 GetCertInitial 是注册的一部分，在轮询期间的消息交换应携带与前一个 PKCSReq 相同的业务 ID 属性。服务端接收到一个与 PKCSReq 不匹配的 GetCertInitial 时，应忽略该请求。

由于此时证书尚未发出，客户端只能使用自己的主体名称（通过 PKCSReq 发送的，包含在 GM/T 0092 格式中的证书注册请求）来识别轮询证书请求。因为来自一个客户端可以有多个未完成的请求（例如，不同的密钥和不同的密钥用法将被用来请求多个证书），事务 ID 也应包括在内，以消除多个请求之间的歧义。

先决条件：客户端已经收到一个事务状态为 PENDING 的 CertRep 消息。

后置条件：客户端已经收到了有效的回复，可以是有效的证书（事务状态为 SUCCESS），也可以申请失败（事务状态为 FAILURE），或者轮询周期超时。

7.3.2 响应消息格式

GetCertInitial 的响应消息与 7.2.2 中相同。

7.4 证书查询

7.4.1 请求消息格式

客户端可以通过签发者名称和待查询证书的证书序列号，从 SCEP 服务端查询签发的证书。此事务不用于提供通用证书目录服务。

此事务由客户端发送到服务端的一个 GetCert 消息，并从服务端得到一个 CertRep 消息作为响应。

先决条件：证书认证机构已发出客户端实体的证书，而签发者指定的序列号是已知的。

后置条件：成功应返回证书，或者请求被拒绝。

7.4.2 响应消息格式

在这种情况下，服务端上的 CertRep 与 7.2.2 相同，只是服务端返回状态只有 SUCCESS 和 FAILURE 两种。

7.5 CRL 查询

7.5.1 请求消息格式

客户端可以从 SCEP 服务端请求 CRL。

先决条件：证书认证机构证书已下载到最终实体。

后置条件:将 CRL 发送回客户端。

7.5.2 响应消息格式

CRL 被通过 CertRep 消息发送回客户端,此消息的信息部分是如 6.4 的一个简化的 SignedData 数据类型,仅包含 CRL。

7.6 获取下一个 CA 证书

7.6.1 请求消息格式

当 CA 证书即将过期时,客户端需要检索 CA 的即将启用的新 CA 证书。这是通过 GetNextCACert 消息完成的,该消息没有相关请求数据。

7.6.2 响应消息格式

响应消息应由 CA 或 RA 签名,客户端应在接受其任何内容之前应先对签名进行验证,签名消息符合 GB/T 35275 中的 SignedData 结构。

SignedData 的内容是简化的,其中包含新的 CA 证书和可能存在的新的 RA 证书,如 8.2.1 中所定义。

如果 CA 没有即将启用的新 CA 证书,则应拒绝该请求,并从功能中删除 GetNextCACert 设置,直到其成功进行证书更新后再恢复设置。

如果此响应中有任何 RA 证书,客户端应检查这些 RA 证书是否由 CA 签名,并且应检查这些 RA 证书的授权。

8 SCEP 传输协议

8.1 HTTP 消息格式

8.1.1 请求消息

SCEP 使用 HTTP "GET"消息实现传输协议。下面定义了从客户端发送到服务端 HTTP GET 消息的语法。

"GET" CGI-PATH CGI-PROG "? operation=" OPERATION "&message=" MESSAGE

其中:

CGI-PATH 定义了调用解析请求 CGI 程序的实际 CGI 路径。

CGI-RROG 被设置为字符串"pkiclient.exe"。这是 CA 用来处理 SCEP 事务的程序。CA 可忽略 CGI-RROG,只使用 CGI-PATH。

OPERATION 和 MESSAGE 取决于具体 SCEP 事务,在以下各条中定义。

如果 CA 支持,则除 GetCACert、GetNextCACert 或 GetCACaps 之外,其他 SCEP 消息都可以不通过 HTTP GET,而通过 HTTP POST 发送。在这种形式的消息中,不使用 base64 编码。

POST /cgi-bin/pkiclient.exe? operation=PKIOperation HTTP/1.0Content-Length:〈length of data〉〈binary GB/T 35275 data〉

客户端可通过 POSTPKIOperation 功能来验证 CA 是否支持 POST 操作,按附录 A 进行。

8.1.2 响应消息

对于每个 GET 操作,CA/RA 服务端应返回内容类型和适当的响应数据。

8.2 SCEP 消息

8.2.1 获取 CA 证书

8.2.1.1 请求消息

OPERATION 应设置为“GetCACert”。

MESSAGE 可省略，也可能是表示证书认证机构签发者标识符的字符串。一个 SCEP 服务端可以支持多个 CA。

8.2.1.2 响应消息

客户端在注册期间，根据 CA 设置的策略与 CA 或 RA 通信。

a) CA 证书响应

响应消息应具有“application/x-x509-ca-cert”的内容类型。

此响应消息的正文仅由 CA 证书组成，如 7.1.2 中所定义。

"Content-Type:application/x-x509-ca-cert\n\n"〈binary X.509〉

b) CA 和 RA 证书响应

响应消息应具有“application/x-x509-ca-ra-cert”的内容类型。

此响应消息的正文由一个简化的数字信封组成，如 7.1.2 中所定义。

"Content-Type:application/x-x509-ca-ra-cert\n\n"〈binary GB/T 35275〉

8.2.2 证书注册

8.2.2.1 请求消息

OPERATION 应设置为“PKIOperation”。

MESSAGE 应设置为 PKCSReq 消息。该消息应按 base64 编码。“base64”编码的数据与“base64url”编码的数据不同，可能包含 URI 保留字符，因此应进行转义。

8.2.2.2 响应消息

响应消息应具有“application/x-pki-message”的内容类型。

此响应消息应为 CertRep 消息，如 7.2.1 中所定义。

"Content-Type:application/x-pki-message\n\n"〈binary CertRep msg〉

8.2.3 证书轮询

8.2.3.1 请求消息

OPERATION 应设置为“PKIOperation”。

MESSAGE 应设置为 GetCertInitial 消息。该消息应按 base64 编码。“base64”编码的数据与“base64url”编码的数据不同，可能包含 URI 保留字符，因此应进行转义。

8.2.3.2 响应消息

此响应消息应设置为 CertRep 消息，如 7.3.1 中定义。

8.2.4 证书查询

8.2.4.1 请求消息

OPERATION 应设置为“PKIOperation”。

MESSAGE 应设置为 GetCert 消息，该消息应按 base64 编码。“base64”编码的数据与“base64url”编码的数据不同，可能包含 URI 保留字符，因此应进行转义。

8.2.4.2 响应消息

此响应消息应设置为 CertRep 消息，如 7.4.1 中定义。

8.2.5 CRL 查询

8.2.5.1 请求消息

OPERATION 应设置为“PKIOperation”。

MESSAGE 应设置为 GetCRL 消息，该消息应按 base64 编码。“base64”编码的数据与“base64url”编码的数据不同，可能包含 URI 保留字符，因此应进行转义。

8.2.5.2 响应消息

此响应消息应设置为 CertRep 消息，如 7.5.1 中定义。

8.2.6 获取下一个 CA 证书

8.2.6.1 请求消息

OPERATION 应设置为“GetNextCACert”。

MESSAGE 可省略，也可以是 CA 管理员设置的证书认证机构标识的字符串。

8.2.6.2 响应消息

响应消息应具有“application/x-x509-next-ca-cert”的内容类型。

该响应正文包含如 7.6.1 部分定义的 GB/T 35275 格式的签名数据。

"Content-Type:application/x-x509-next-ca-cert\n\n"〈binary GB/T 35275〉

附 录 A
（规范性）
GetCACaps 消息

A.1 GetCACaps 请求消息

GetCACaps 消息请求获取 CA 的功能，CA 应支持 GetCACaps 消息。其语法格式为：
"GET" CGI-PATH CGI-PROG "？operation＝GetCACaps""&message＝" CA-IDENT

A.2 GetCACaps 功能响应格式

GetCACaps 消息的响应是 CA 功能的列表，由〈LF〉字符分隔的纯文本，见表 A.1。

表 A.1 CA 功能列表

关键词	描述
GetNextCACert	CA 支持 GetNextCACert 消息
POSTPKIOperation	PKIOPeration 消息可以通过 HTTP POST 传送
Renewal	客户端可以使用当前证书和密钥来验证新证书的注册请求
SM3	CA 支持 SM3 算法
SM4	CA 支持 SM4 算法

服务端应使用此处指定的文本大小写，但在处理此消息时，客户端应忽略文本大小写。客户端应能够接受和忽略可能由 CA 发送回的任何未知关键字。

如果 CA 不支持上述任何功能，应返回空消息或 HTTP 错误。接收空消息或 HTTP 错误的客户端应将响应解释为 CA 不支持任何请求的功能。

参 考 文 献

[1] RFC2315 PKCS #7: Cryptographic Message SyntaxVersion 1.5

[2] RFC2986 PKCS #10: Certification Request Syntax Standard Version 1.7

[3] RFC4648:The Base16, Base32, and Base64 Data Encodings

[4] Internet Engineering Task Force, Internet-Draft, Simple Certificate Enrollment Protocol, draft-nourse-scep-23

中华人民共和国密码
行业标准
简单证书注册协议规范
GM/T 0089—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 1.5 字数 42 千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35971 定价 26.00 元

GM/T 0089-2020

码上扫一扫 正版服务到