简单证书注册协议概述

目录

简介
背景信息
CA身份验证
请求
回复
客户注册
请求
回复
客户端重新注册
续约
滚动
构建块
PKCS#7
签名信封(SignedData)
封装数据(EncoledData)
PKCS#10
相关信息
Appendix
SCEP请求
请求消息格式
示意性视图
SCEP响应
响应消息格式
内容类型
pkiMessage结构
SCEP OID
SCEP pkiMessage
SCEP消息类型
SCEP pkiStatus

简介

本文档介绍简单证书注册协议(SCEP)，该协议用于注册和其他公钥基础设施(PKI)操作。

背景信息

SCEP最初由思科开发，并记录在互联网工程任务组(IETF)草案中。

其主要特点是：

- 基于HTTP的请求/响应模型(GET方法；POST方法的可选支持)
- 仅支持基于RSA的加密
- 使用PKCS#10作为证书请求格式
- 使用PKCS#7传输加密签名/加密消息
- 支持服务器通过请求方定期轮询进行异步授权
- 具有有限的证书撤销列表(CRL)检索支持(出于可扩展性原因，首选方法是通过CRL分发点(CDP)查询)
- 不支持在线证书撤销（必须通过其他方式离线完成）
- 要求在证书签名请求(CSR)中使用质询密码字段，该字段必须仅在服务器和请求方之间共享

SCEP的注册和使用通常遵循以下工作流程：

1. 获取证书颁发机构(CA)证书的副本并进行验证。
2. 生成CSR并将其安全发送到CA。
3. 轮询SCEP服务器以检查证书是否已签名。
4. 根据需要重新注册，以在当前证书到期之前获得新证书。
5. 根据需要检索CRL。

CA身份验证

SCEP使用CA证书来保护CSR的消息交换。因此，必须获取CA证书的副本。使用GetCACert操作。

请求

请求作为HTTP GET请求发送。请求的数据包捕获类似于以下内容：

```
GET /cgi-bin/pkiclient.exe?operation=GetCACert
```

回复

响应仅是二进制编码CA证书(X.509)。 客户端需要通过检查指纹/哈希来验证CA证书是否受信任。这必须通过带外方法（向系统管理员打电话或在信任点内预配置指纹）来完成。

客户注册

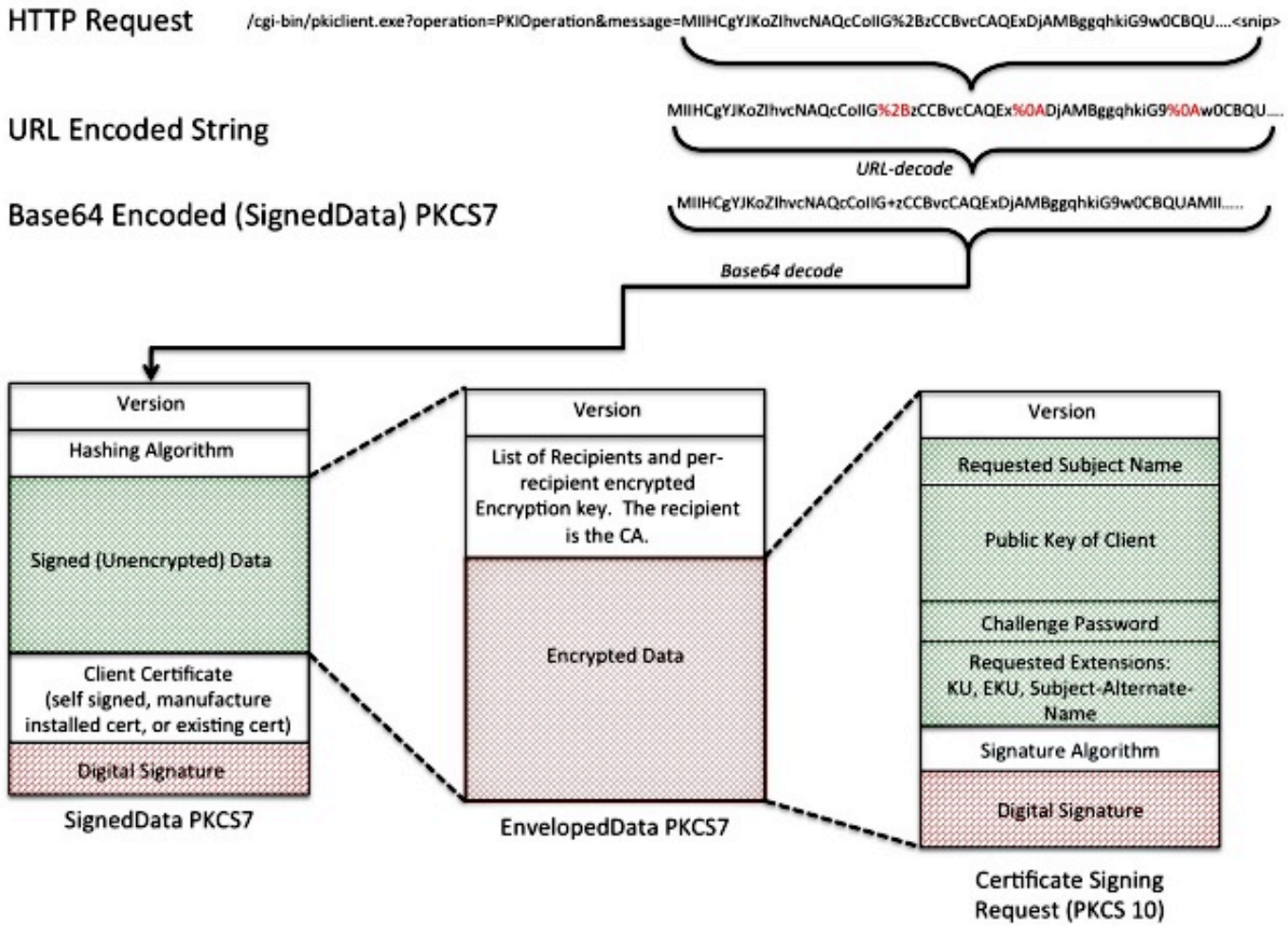
请求

注册请求作为HTTP GET请求发送。该请求的数据包捕获类似于以下内容：

```
/cgi-bin/pkiclient.exe?operation=PKIOperation&message=
MIIHCgYJKoZIhvcNAQcCoIIG%2BzCCBvcCAQExDjA......<snip>
```

1. "message="后面的文本是URL编码字符串，从GET请求字符串中提取。
2. 然后，文本将URL解码为ASCII文本字符串。该文本字符串是Base64编码的SignedData PKCS#7。
3. SignedData PKCS#7由客户端用其中一个证书签名；它用于证明客户端发送了它，并且它在传输中未被更改：
   自签名证书（在初始注册时使用）制造商安装的证书(MIC)即将到期的当前认证（重新注册）

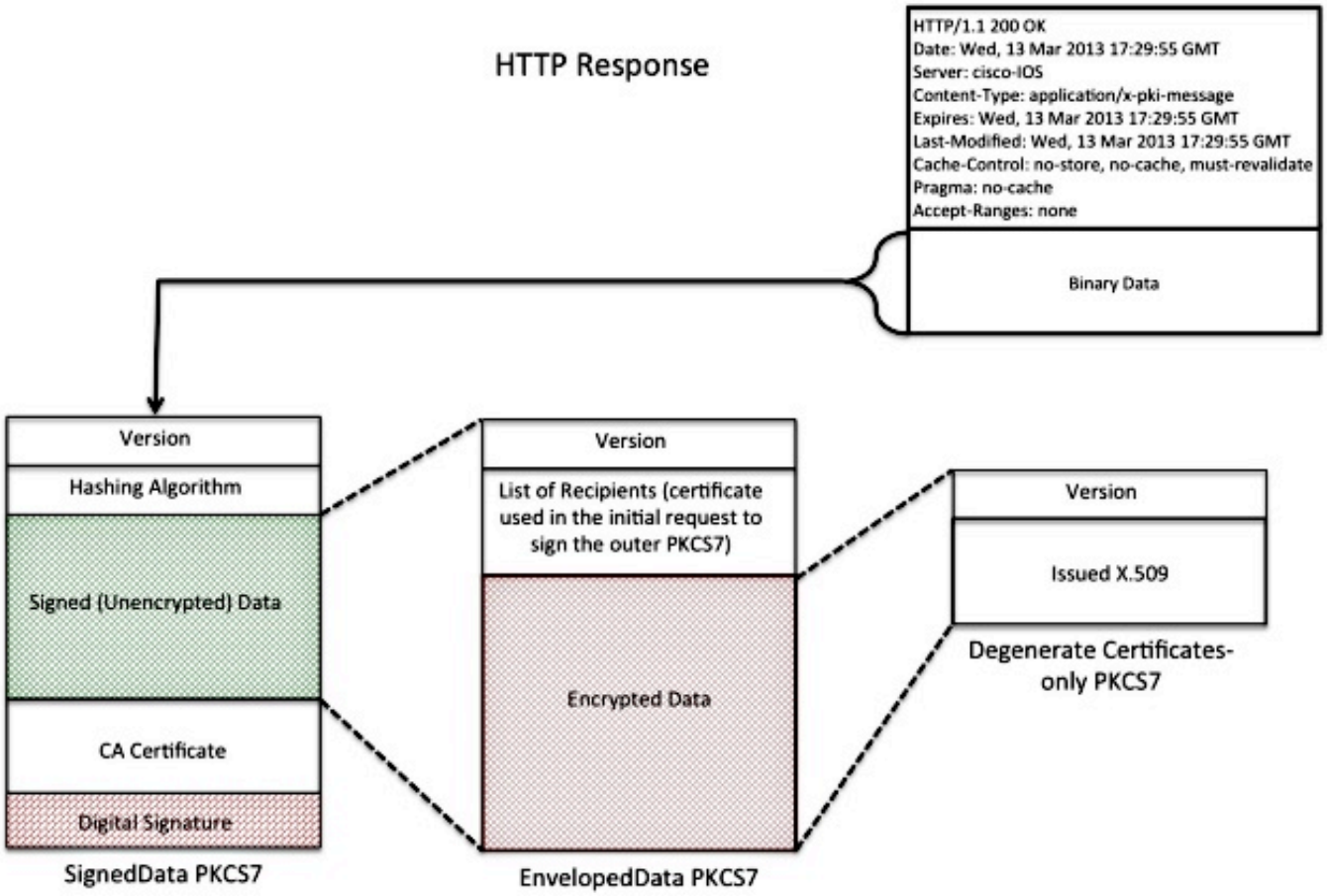
4. SignedData PKCS#7的“Signed Data”部分是EncapledData PKCS#7。
5. EncoveledData PKCS#7是包含“加密数据”和“解密密钥”的容器。 解密密钥使用收件人的公钥加密。在此特定情况下，收件人是CA;因此，只有CA才能实际解密“加密数据”。
6. 已包络PKCS#7的“加密数据”部分是CSR(PKCS#10)。



回复

对SCEP注册请求的响应是以下三种类型之一：

- **拒绝** — 管理员因以下原因拒绝请求：
  密钥大小无效无效的质询密码CA无法验证请求请求要求提供CA未授权的属性请求由CA不信任的身份签名
- **待**处理 — CA管理员尚未审核请求。
- **成功** — 请求被接受，并且签名证书被包括。签名证书保留在称为“简并仅证书PKCS#7”的特殊类型的PKCS#7中，该特殊容器可以容纳一个或多个X.509或CRL，但不包含签名或加密数据负载。



客户端重新注册

在证书到期之前，客户端需要获取新证书。续约和翻转之间存在细微的行为差异。当客户端的ID证书即将到期，且其到期日期与CA证书的到期日期不同（早于）时，会发生续订。当ID证书即将到期且其到期日期与CA的证书到期日期相同时，将发生滚动更新。

续约

随着ID证书到期日期的临近，SCEP客户端可能希望获取新证书。客户端生成CSR并完成注册流程（如前所定义）。 当前证书用于签名SignedData PKCS#7，这反过来证明CA的身份。收到新证书后，客户端立即删除当前证书并将其替换为新证书，新证书的有效性立即开始。

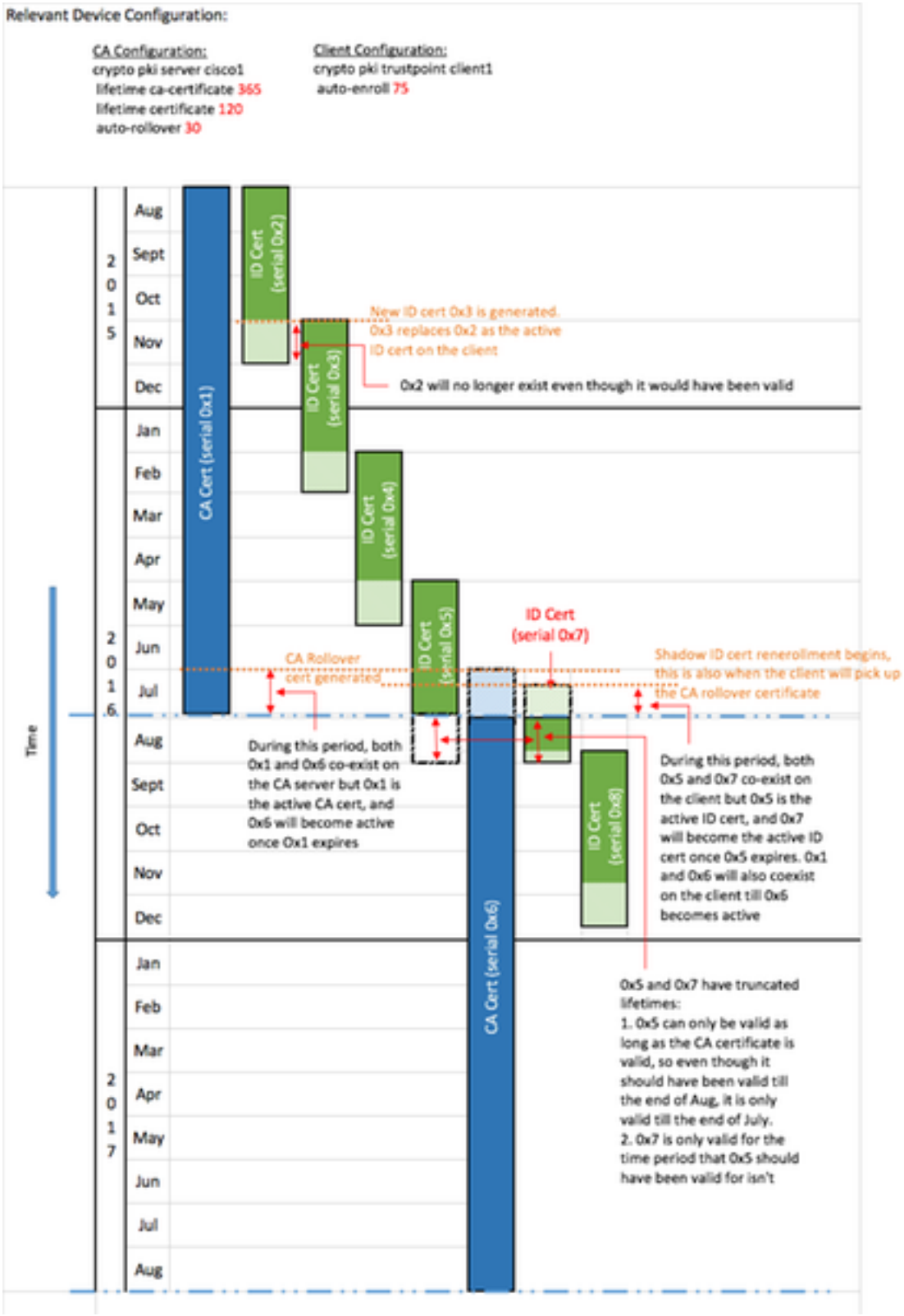
滚动

滚动更新是CA证书过期并生成新CA证书的特殊情况。CA生成新的CA证书，当前CA证书过期后，该证书将生效。CA通常会在滚动更新时间之前的某个时间生成此“影子CA”证书，因为为了为客户端生成“影子ID”证书，需要生成该证书。

当SCEP客户端的ID证书即将到期时，SCEP客户端会向CA查询“影子CA”证书。此操作通过GetNextCACert**操作完**成，如下所示：

```
GET /cgi-bin/pkiclient.exe?operation=GetNextCACert
```

一旦SCEP客户端拥有“影子CA”证书，它会在正常注册过程后请求“影子ID”证书。CA使用“Shadow CA”证书签署“Shadow ID”证书。与正常续约请求不同，返回的“影子ID”证书在CA证书到期（滚动）时生效。 因此，客户端需要为CA和ID证书保留滚动前和滚动后证书的副本。在CA到期（全反）时，SCEP客户端删除当前CA证书和ID证书，并用“卷影”副本替换它们。



构建块

此结构用作SCEP的构建块。

注意：PKCS#7和PKCS#10不特定于SCEP。

PKCS#7

PKCS#7是允许对数据签名或加密的已定义数据格式。数据格式包括执行加密操作所需的原始数据和相关元数据。

签名信封(SignedData)

签名信封是一种格式，用于传送数据并确认封装的数据在传输过程中没有通过数字签名进行更改。包括以下信息：

```
SignedData &colon;:= SEQUENCE {
version CMSVersion,
digestAlgorithms DigestAlgorithmIdentifiers,
encapContentInfo EncapsulatedContentInfo,
certificates [0] IMPLICIT CertificateSet OPTIONAL,
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
signerInfos SignerInfos }
```

- 版本号 — 使用SCEP时，使用第1版。
- 使用的摘要算法列表 — 对于SCEP，只有一个签名者，因此只有一个散列算法。
- 已签名的实际数据 — 使用SCEP，这是PKCS#7 Enveloped-data格式（加密信封）。
- 签名者证书列表 — 使用SCEP，这是初始注册时的自签名证书，或当您重新注册时的当前证书。
- 签名者列表和每个签名者生成的指纹 — 使用SCEP时，只有一个签名者。

封装的数据未加密或模糊处理。此格式仅提供对已更改消息的保护。

封装数据(EncoledData)

“封装数据”格式传送已加密且只能由指定收件人解密的数据。 包括以下信息：

```
EnvelopedData &colon;:= SEQUENCE {
version CMSVersion,
originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
recipientInfos RecipientInfos,
encryptedContentInfo EncryptedContentInfo,
unprotectedAttrs [1] IMPLICIT UnprotectedAttributes OPTIONAL }
```

- 版本号 — 使用SCEP时，使用版本0。
- 每个收件人的列表和相关加密数据加密密钥 — 使用SCEP时，只有一个收件人(对于请求：CA服务器；对于回复：客户端)。
- 加密数据 — 此数据使用随机生成的密钥加密（已使用收件人的公钥加密）。

PKCS#10

PKCS#10描述CSR的格式。CSR包含客户端请求包含在其证书中的信息：

- 主题名称
- 公钥的副本
- 质询密码（可选）

- 请求的任何证书扩展，例如：
  密钥使用(KU)扩展密钥使用(EKU)主题备用名称(SAN)通用主体名称(UPN)
- 请求的指纹

以下是CSR的示例：

```
Certificate Request:
Data&colon;
Version: 0 (0x0)
Subject: CN=scepclient
Subject Public Key Info:

Public Key Algorithm: rsaEncryption Public-Key: (1024 bit)
Modulus:
00:cd:46:5b:e2:13:f9:bf:14:11:25:6d:ff:2f:43:
64:75:89:77:f6:8a:98:46:97:13:ca:50:83:bb:10:
cf:73:a4:bc:c1:b0:4b:5c:8b:58:25:38:d1:19:00:
a2:35:73:ef:9e:30:72:27:02:b1:64:41:f8:f6:94:
7b:90:c4:04:28:a1:02:c2:20:a2:14:da:b6:42:6f:
e6:cb:bb:33:c4:a3:64:de:4b:3a:7d:4c:a0:d4:e1:
b8:d8:71:cc:c7:59:89:88:43:24:f1:a4:56:66:3f:
10:25:41:69:af:e0:e2:b8:c8:a4:22:89:55:e1:cb:
00:95:31:3f:af:51:3f:53:ad
Exponent: 65537 (0x10001)
Attributes:
challengePassword :
Requested Extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Subject Alternative Name:
DNS:webserver.example.com
Signature Algorithm: sha1WithRSAEncryption
8c:d6:4c:52:4e:c0:d0:28:ca:cf:dc:c1:67:93:aa:4a:93:d0:
d1:92:d9:66:d0:99:f5:ad:b4:79:a5:da:2d:6a:f0:39:63:8f:
e4:02:b9:bb:39:9d:a0:7a:6e:77:bf:d2:49:22:08:e2:dc:67:
ea:59:45:8f:77:45:60:62:67:64:1d:fe:c7:d6:a0:c3:06:85:
e8:f8:11:54:c5:94:9e:fd:42:69:be:e6:73:40:dc:11:a5:9a:
f5:18:a0:47:33:65:22:d3:45:9f:f0:fd:1d:f4:6f:38:75:c7:
a6:8b:3a:33:07:09:12:f3:f1:af:ba:b7:cf:a6:af:67:cf:47: 60:fc
```

相关信息

- SCEP IETF草案
- 使用CLI配置指南的传统SCEP
- 为BYOD配置SCEP支持

Appendix

SCEP请求

请求消息格式

请求以HTTP GET形式发送：

```
GET CGI-path/pkiclient.exe?operation=operation&message=message HTTP/version
```

其中：

- **CGI-path依**赖于服务器，并指向处理SCEP请求的通用网关接口(CGI)程序： Cisco IOS® CA使用空路径字符串。Microsoft CA使用**/certsrv/mscep/mscep.dll**，它指向MSCEP/网络设备注册服务(NDES)IIS服务。
- **操作**标识要执行的操作。
- **消息**为该操作传送其他数据（如果不需要实际数据，则该消息可为空）。

使用GET方法时，消息部分为纯文本或转换为Base64的由可分辨编码规则(DER)编码的PKCS#7。如果支持POST方法，则将使用GET的Base64编码发送的内容可以使用POST以二进制格式发送。

示意性视图

操作及其**关联**的消息值**的可**能值：

- **操作=** `PKIOperation`: **邮件**是基于PKCS#7的SCEP **pkiMessage**结构，并使用DER和Base64编码。**pkiMessage**结构可以有以下类型： **PKCSReq**:PKCS#10 CSR**GetCertInitial**:轮询CSR授予状态**GetCert**或**GetCRL**:证书或CRL检索
- **operation = GetCACert、 GetNextCACert** 或（可选）**GetCACaps**: **消**息可以省略，也可以设置为标识CA的名称。

SCEP响应

响应消息格式

SCEP响应作为标准HTTP内容返回，其内容类**型取决于**原始请求和返回的数据类型。DER内容以二进制形式返回（对于请求，不在Base64中）。PKCS#7内容可能包含加密/签名的封装数据；如果它不包含（仅包含一组证书），则称为**退化**PKCS#7。

内容类型

Content-Type的可**能值**:

application/x-pki-message:

- 响应PKIOperation**操作**，使用**pkiMessage**类型：**PKCSReq、GetCertInitial、GetCert或GetCRL**
- 响应正文是**pkiMessage**的类型：**CertRep**

application/x-x509-ca-cert:

- 响应GetCACert**操**作
- 响应正文是DER编码的X.509 CA证书

application/x-x509-ca-ra-cert:

- 响应GetCACert**操**作
- 响应正文是DER编码的简并PKCS#7，包含CA和RA证书

application/x-x509-next-ca-cert:

- 响应GetNextCACert操作
- 响应体是pkiMessage类型的变体：CertRep

pkiMessage结构

SCEP OID

```
2.16.840.1.113733.1.9.2 scep-messageType
2.16.840.1.113733.1.9.3 scep-pkiStatus
2.16.840.1.113733.1.9.4 scep-failInfo
2.16.840.1.113733.1.9.5 scep-senderNonce
2.16.840.1.113733.1.9.6 scep-recipientNonce
2.16.840.1.113733.1.9.7 scep-transId
2.16.840.1.113733.1.9.8 scep-extensionReq
```

SCEP pkiMessage

- PKCS#7 SignedData(PKCS#7签名数据)
- PKCS#7 EnvelopedData(称为pkcsPKIEnvelope;可选，加密到邮件收件人)
  messageData（CSR、证书、CRL...）
- SignerInfo和authenticatedAttributes:
  transactionID、messageType、senderNoncepkiStatus、recipientNonce（仅响应）failInfo（仅响应+失败）

SCEP消息类型

- 请求：
  PKCSReq(19):PKCS#10 CSRGetCertInitial(20):证书注册轮询GetCert(21):证书检索
  GetCRL(22):CRL检索
- 回复：
  CertRep(3):对证书或CRL请求的响应

SCEP pkiStatus

- 成功(0):请求已授予（pkcsPKIEnvelope中的响应）
- 故障(2):请求被拒绝（失败信息属性中的详细信息）
- 待处理(3):请求等待手动审批