简单认证登记协议概述

目录

简介

本文描述简单认证登记协议(SCEP)，是用于登记和其他公共密钥基础设施(PKI)操作的协议。

背景信息

SCEP由思科在互联网工程任务组(IETF)草稿最初开发和描述。

其主要特性是：

- 根据HTTP的请求/响应型号(GET方法;POST方法的可选技术支持)
- 仅支持RSA根据加密算法
- 使用PKCS-10作为证书请求格式
- 使用PKCS-7为了转达密码签字/加密的消息
- 由服务器支持异步授权，有正常?的由请求方
- 限制了证书撤销列表(CRL)检索支持(首选方法是通过控制分配点(CDP)查询，可扩展性原因的)
- 不支持联机认证吊销(必须是执行的脱机通过其它方法)
- 要求使用在证书签名请求(CSR)内的一**Challenge Password字段**，必须仅共享在服务器和请求方之间

SCEP登记和使用情况通常跟随此工作流程：

1. 得到Certificate Authority (CA)证书的复制并且验证它。
2. 生成CSR并且安全地发送它对CA。
3. 轮询SCEP服务器为了证实证书是否签了字。
4. 如所需要重新登记为了在当前证书的有效期之前获取新证书。
5. 如所需要获取CRL。

CA认证

SCEP使用CA证书为了获取CSR的消息交换。结果，得到CA证书的复制是必要的。使用**GetCACert**操作。

请求

请求发送作为HTTP GET请求。请求的一数据包捕获看起来类似于此：

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

答复

答复是二进制编码的CA证书(X.509)。客户端需要验证CA证书通过指纹/哈希的考试委托。这必须通过指纹的带外方法(对系统管理员的一部电话或预配置在信任点内的执行)。

客户注册

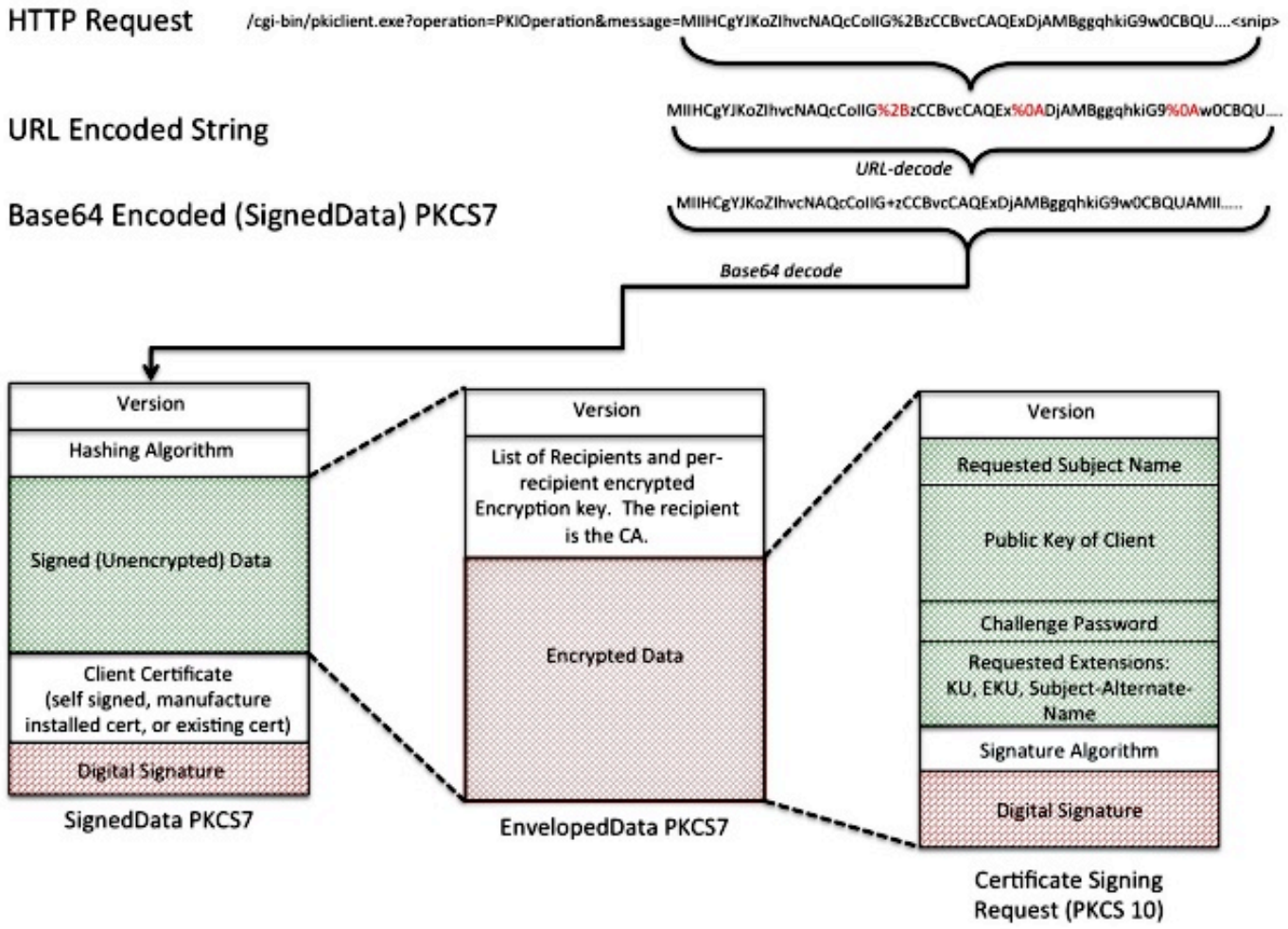
请求

注册请求发送作为HTTP GET请求。 请求的一数据包捕获看起来类似于此：

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

1. 文本，在“message=”是URL编码的字符串后，从GET请求字符串解压缩。
2. 文本是然后URL解码到ASCII文本字符串。该文本字符串是Base64-encoded SignedData PKCS-7。
3. SignedData PKCS-7由有这些证书之一的客户端签字;用于证明，客户端发送它，并且在运送中未被修改：
   自签名证书(使用在最初的登记)制造商预装证书(MIC)很快超时的一个当前证明(重新登记)

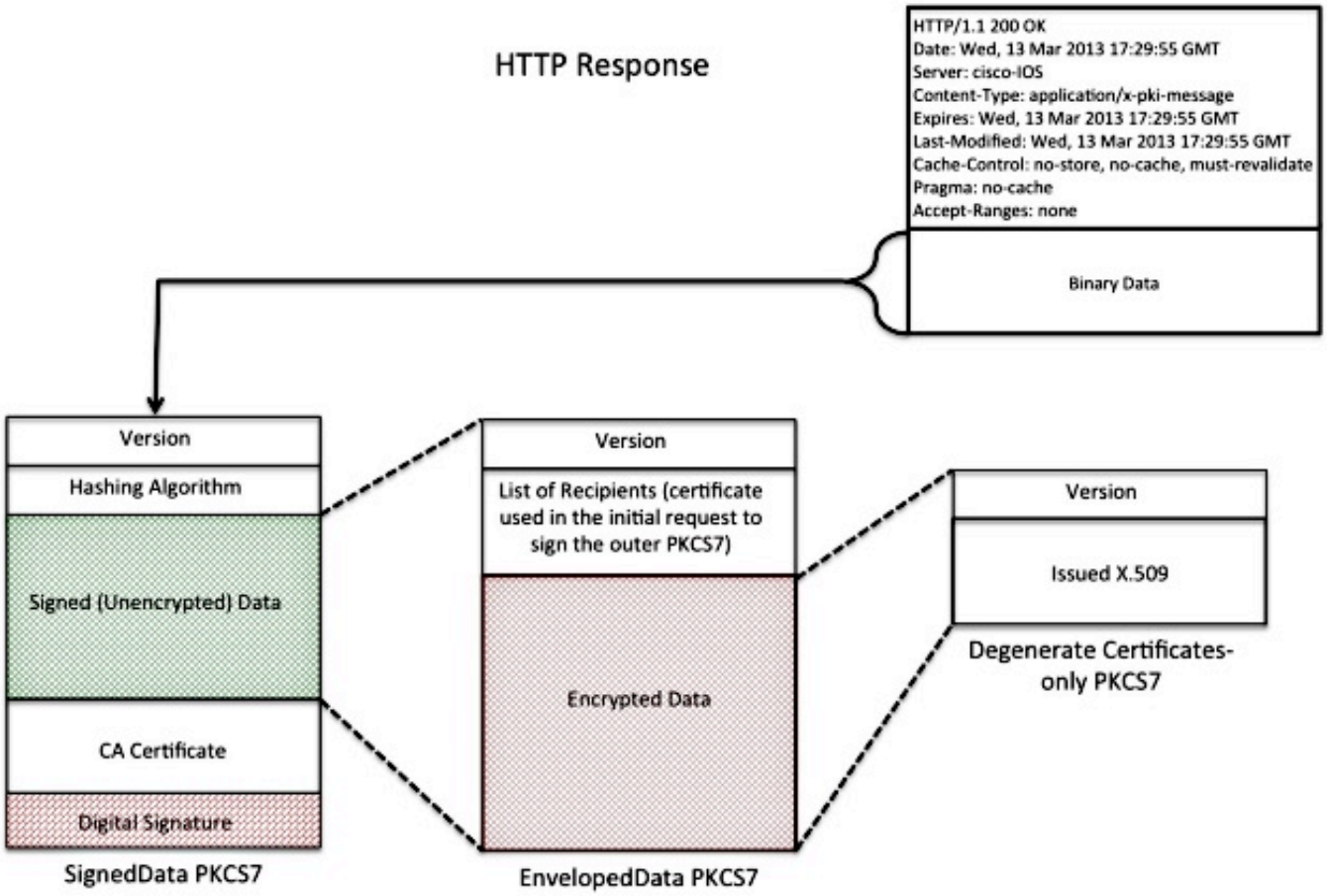
4. SignedData PKCS-7的“签名数据”部分是EnvelopedData PKCS-7。
5. EnvelopedData PKCS-7是包含“已加密数据”的容器和“解密密钥”。解密密钥用收件人的公共密钥加密。对这个特殊情况，收件人是CA;结果。仅CA能实际上解密“已加密数据”。
6. 被包围的PKCS-7的“已加密数据”部分是CSR (PKCS-10)。



答复

对SCEP注册请求的答复是三个类型之一：

- **拒绝**-请求由任何数量的原因的管理员拒绝，例如：
  无效密钥大小无效私钥保护密码CA不能验证请求请求为CA没有授权的属性询问请求由CA不委托的标识签字
- **等待**- CA管理员未查看请求。
- **成功**-请求接受，并且签名证书包括。签名证书在保持呼叫的PKCS-7内特殊类型是一个特殊容器能保持一个或更多X.509或Crl，但是不包含一签字的或已加密数据有效负载的“退化仅使用证书的PKCS#7,"。



客户端重新登记

在证书到期之前，客户端需要获得新证书。有在续订和反转之间的一个轻微的性能上的区别。续订发生，当客户端的ID证书接近有效期，并且其有效期不是相同的(早于)象CA证书的有效期。反转发生，当ID证书接近有效期，并且其有效期是相同的象CA的证书到期到期日。

续订

因为ID证书的有效期接近， SCEP客户端也许要获取新证书。客户端生成CSR并且通过登记进程(如以前定义)。当前证书用于为了签署SignedData PKCS-7，反过来证明标识对CA.收到新证书后，客户端立即删除当前证书并且用新的替换它，立即有效性开始。

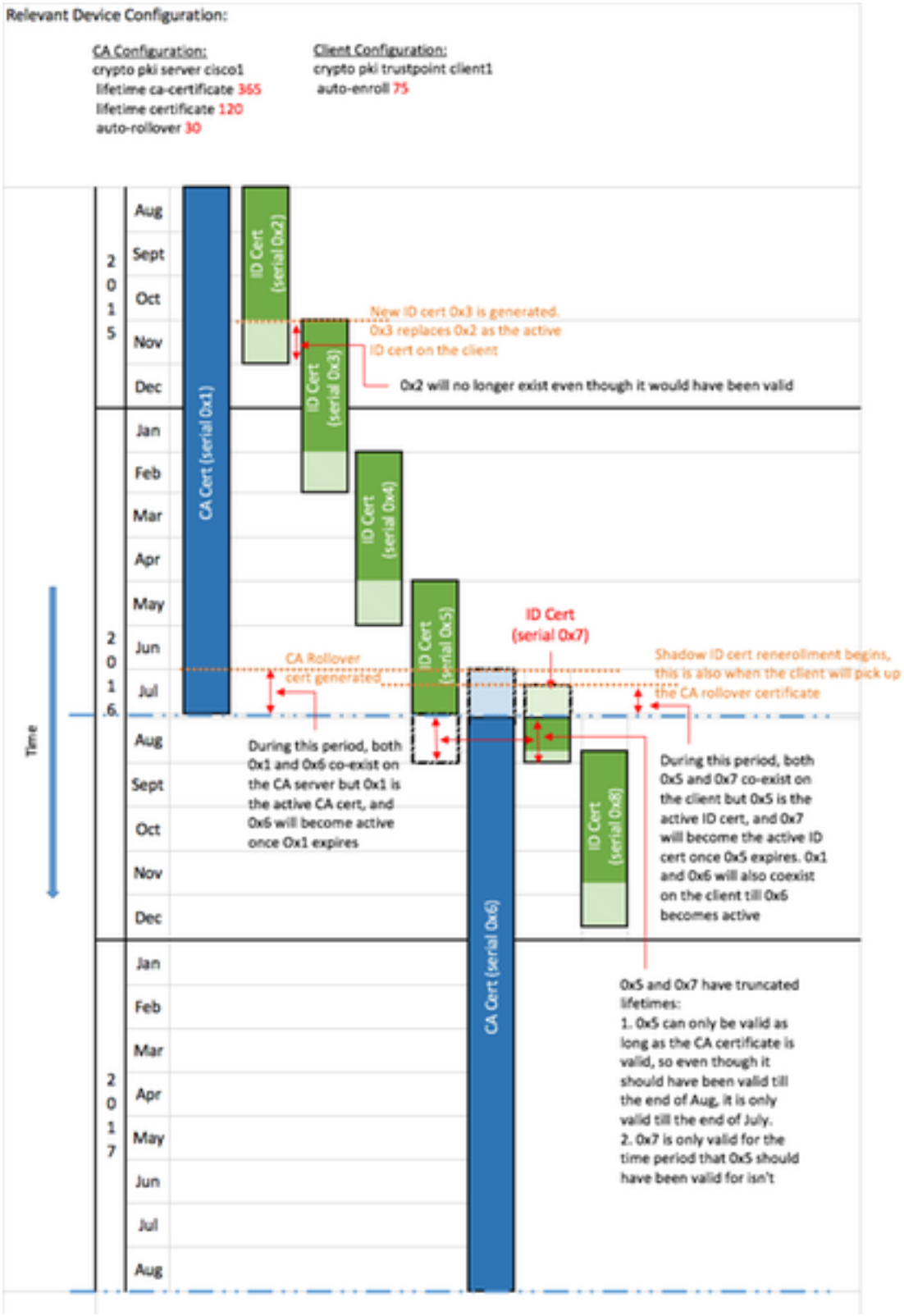
反转

反转是CA证书超时的特殊情况，并且一个新的CA证书生成。CA生成变得有效当前CA证书一次超时的一个新的CA证书。因为是需要的为了生成“Shadow客户端的， ID”证书CA在反转时间之前通常生成此“Shadow CA”证书一些时间。

当SCEP客户端ID证书接近有效期， SCEP客户端查询“Shadow CA”证书的CA。这执行与**GetNextCACert**操作如显示此处：

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

一旦SCEP客户端有“Shadow CA”证书，在正常登记程序以后请求“Shadow ID”证书。CA签署与“Shadow CA”证书的“Shadow ID”证书。不同于一正常续订请求，返回的“Shadow ID”证书变得有效在CA证书有效期(反转)时。结果，客户端需要保留前和POST反转证书的复制CA和ID证书的。在CA有效期(反转)时， SCEP客户端删除当前CA证书和ID证书并且用“Shadow”复制替换他们。



构建模块

此结构使用作为SCEP构建模块。

Note:PKCS-7和PKCS-10不是SCEP特定。

PKCS-7

PKCS-7是允许将签字或加密的数据的定义数据格式。数据格式包括的原始数据和必要相关的元数据为了执行密码操作。

署名的信封(SignedData)

署名的信封是传送数据的格式并且确认封装的数据在运送中没有通过数字签名被修改。它包括此信息：

```
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，使用的版本1。
- 摘要算法列表使用的-使用SCEP，只只有一个签署人和因而一哈希算法。
- 签字的实际数据-使用SCEP，这是PKCS-7包围数据格式(已加密信封)。
- 签署人的证书列表-使用SCEP，如果再登记，这是在最初的登记的一自签名证书或当前证书。
- 每个签署人和指纹的生成的列表签署人-有SCEP的，只有一个签署人。

被封装的数据没有加密也没有被弄暗淡。此格式提供防护被修改的消息。

被包围的数据(EnvelopedData)

被包围的数据格式传送加密并且可能由指定的接收方只解密的数据。它包括此信息：

```
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，使用版本0。
- 其中每一的列表个收件人和相关已加密数据加密键-有SCEP的，只有一收件人(请求：CA服务器;答复：客户端)。
- 已加密数据-这加密与用收件人的公共密钥加密)的一随机地生成的密钥(。

PKCS-10

PKCS-10描述CSR的格式。CSR包含客户端要求在他们的证书内包括的信息：

- 主题名称
- 公共密钥的复制
- 私钥保护密码(可选)
- 任何证书扩展reqested，例如：

密钥用法(KU)延长的密钥用法(EKU)附属的替代方案名称(SAN)通用主体名称(UPN)

- 请求的指纹

这是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
- 传统SCEP使用CLI配置指南
- 配置BYOD的SCEP支持

附录

SCEP请求

Request信息格式

请求用表的HTTP GET传送：

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

Where:

- **CGI PATH**依靠服务器和点对处理SCEP请求的通用网关接口(CGI)程序： Cisco IOS CA使用一空路径字符串。Microsoft CA使用**/certsrv/mscep/mscep.dll**，对MSCEP/网络设备登记的点服务(NDES) IIS服务。
- **操作**识别被执行的操作。
- **消息**运载该操作(和它的其它数据可以是空的，如果实际数据没有要求)。

使用GET方法，文电分段是纯文本或者著名的编码规则(DER) -编码的PKCS-7转换对Base64。如果在编码与GET的Base64在与POST的二进制格式将发送也许发送支持的POST方法，请满意。

概要视图

操作和他们相关的**消息**值的可能的值：

- **操作=** `PKIOperation` ： **messageis**一个SCEP **pkiMessage**结构，根据PKCS-7和编码与DER和Base64。**pkiMessage**结构可以是这些类型： **PKCSReq** ：PKCS-10 CSR**GetCertInitial** ：轮询授权状态的CSR的**GetCert**或**GetCRL** ：证书或CRL检索
- **操作= GetCACert**、**GetNextCACert**或者(可选) **GetCACaps** ： **消息**省略或者可以设置为识别CA的名称。

SCEP答复

响应消息格式

SCEP答复返回作为标准HTTP内容，与取决于原始请求和返回的数据种类的**内容类型**。DER内容返回作为二进制(不在Base64至于请求的)。PKCS-7满意也许或也许不包含已加密/签字的被包围的数据;如果它不(只包含一套证书)，指一**退化的**PKCS-7。

内容类型

内容类型的可能的值：

application/x pki消息：

- 以回应**PKIOperation**操作，与类型**pkiMessage** ：**PKCSReq**、**GetCertInitial**、**GetCert**或者**GetCRL**
- 答复正文是类型**pkiMessage** ：**CertRep**

application/x-x509-ca-cert ：

- 以回应**GetCACert**操作
- 答复正文是DER编码的X.509 CA证书

application/x-x509-ca-ra-cert ：

- 以回应**GetCACert**操作
- 答复正文是包含CA和RA证书的一DER编码的退化的PKCS-7

application/x-x509-next-ca-cert ：

- 以回应**GetNextCACert**操作

- 答复正文是类型**pkiMessage的**变化：**CertRep**

pkiMessage结构

SCEP OIDs

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

SCEP pkiMessage

- PKCS-7 **SignedData**
- PKCS-7 EnvelopedData (呼叫**pkcsPKIEnvelope**;可选，已加密对留言收件人)
  messageData (CSR、cert， CRL，…)
- 与**authenticatedAttributes的SignerInfo** ：
  transactionID， **messageType**， **senderNoncepkiStatus**， **recipientNonce** (仅答复)**failInfo** (仅答复+失败)

SCEP messageType

- 请求：
  PKCSReq (19) ：PKCS-10 CSR**GetCertInitial** (20) ：证书登记?**GetCert** (21) ：证书检索
  GetCRL (22) ：CRL检索
- 答复：
  CertRep (3) ：对证书或CRL请求的答复

SCEP pkiStatus

- **成功**(0) ：授权的请求(在pkcsPKIEnvelope的答复)
- **失败**(2) ：拒绝的请求(在Failinfo属性的详细信息)
- **等待**(3) ：请求等候手工的批准