簡單證書註冊協定概述

目錄

簡介

本檔案介紹簡單憑證註冊通訊協定(SCEP)，這是用於註冊和其他公開金鑰基礎架構(PKI)運作的通訊協定。

背景資訊

SCEP最初由思科開發，並記錄在Internet工程任務組(IETF)草案中。

其主要特點是：

- 基於HTTP(GET)方法的請求/響應模型；可選支援POST方法)
- 僅支援基於RSA的加密
- 使用PKCS#10作為證書請求格式
- 使用PKCS#7傳輸加密簽名/加密的郵件
- 支援伺服器的非同步授予，並由請求者定期輪詢
- 具有有限的證書撤銷清單(CRL)檢索支援(出於可擴充性的原因，首選方法是通過一個CRL分發點(CDP)查詢)
- 不支援線上證書吊銷（必須通過其他方式離線完成）
- 要求使用證書簽名請求(CSR)中的**challenge password**欄位，該欄位必須僅在伺服器和請求者之間共用

SCEP的註冊和使用通常遵循以下工作流程：

1. 獲取證書頒發機構(CA)證書的副本並進行驗證。
2. 產生CSR並將其安全傳送到CA。
3. 輪詢SCEP伺服器以檢查證書是否已簽名。
4. 重新註冊，以在當前證書到期之前獲取新證書。
5. 根據需要檢索CRL。

CA驗證

SCEP使用CA憑證以保護CSR的訊息交換。因此，必須獲取CA證書的副本。使用**GetCACert**操作。

請求

請求將作為HTTP GET請求傳送。該請求的資料包捕獲方式如下所示：

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

響應

響應只是二進位制編碼的CA證書(X.509)。 客戶端需要通過檢查指紋/雜湊來驗證CA證書是否受信任。這必須通過帶外方法（通過電話呼叫系統管理員或在信任點內預配置指紋）完成。

客戶端註冊

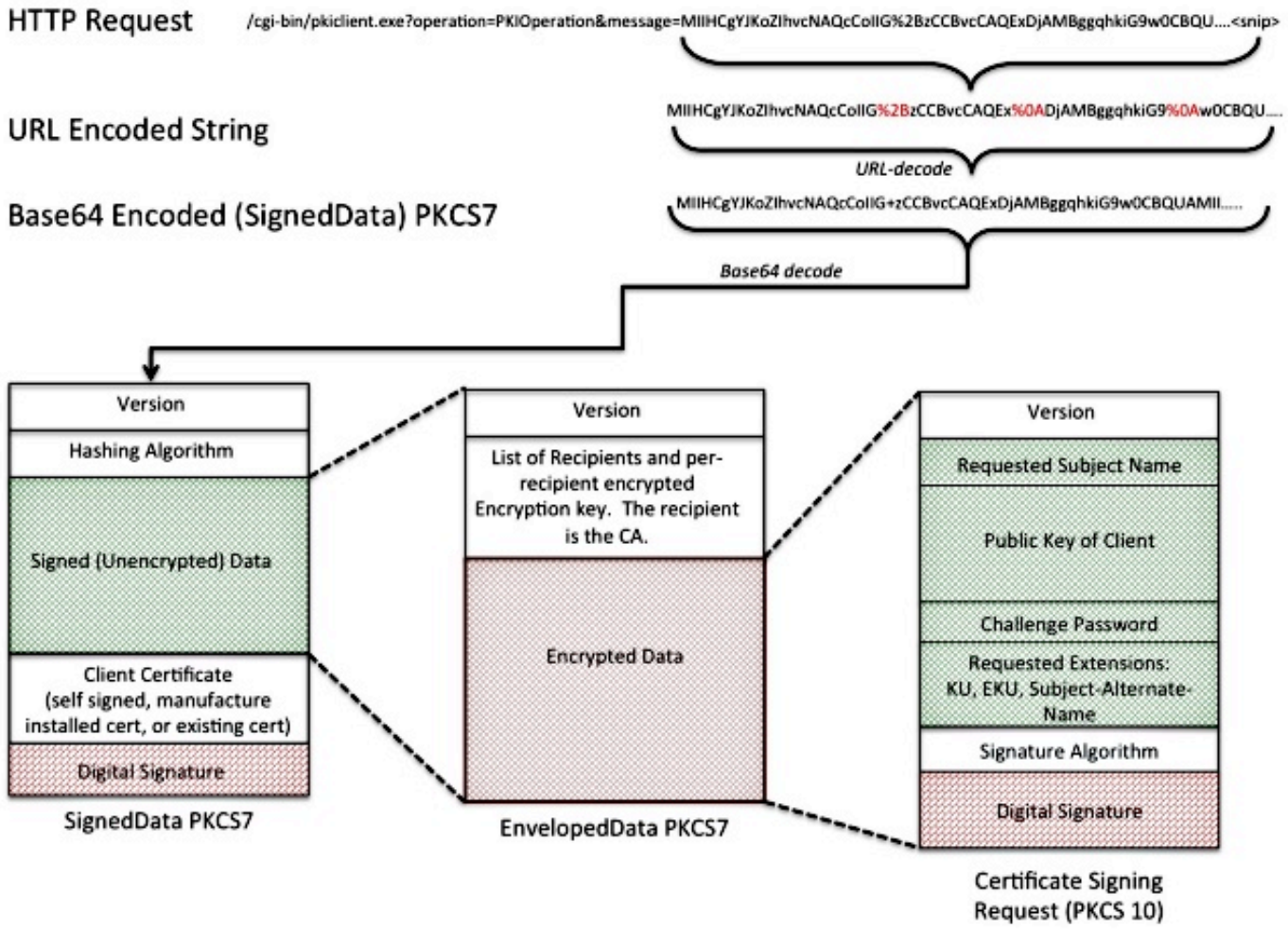
請求

註冊請求將作為HTTP GET請求傳送。該請求的資料包捕獲如下所示：

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

1. 「message=」之後的文本是URL編碼字串，它從GET請求字串中提取。
2. 然後將文本的URL解碼為ASCII文本字串。該文本字串是Base64編碼的SignedData PKCS#7。
3. SignedData PKCS#7由客戶端使用以下證書之一進行簽名；它用於證明客戶端傳送了該資料包，並且傳輸過程中未對其進行更改：

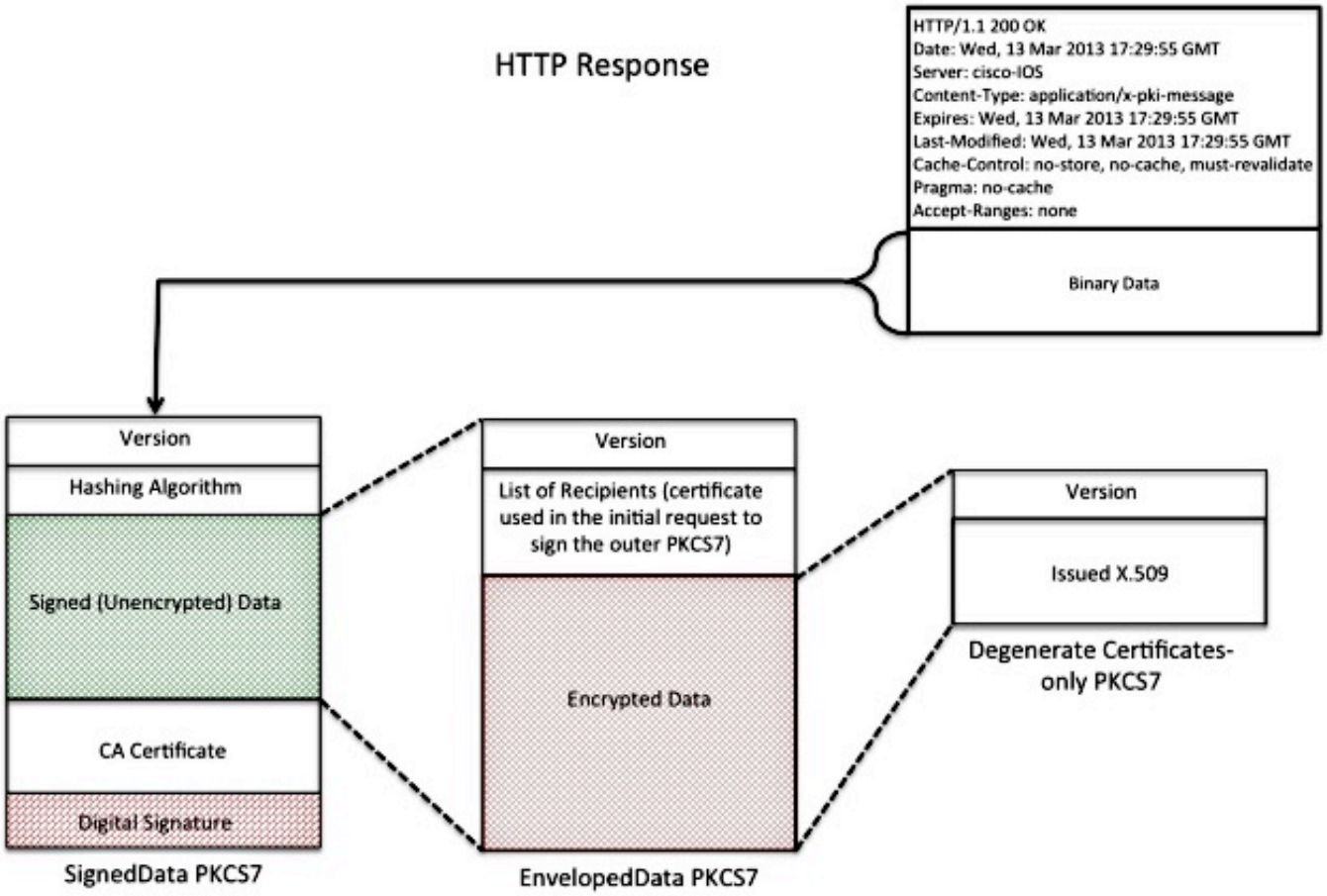
自簽名證書（在初始註冊時使用）製造商安裝的證書(MIC)即將到期的當前證書（重新註冊）
4. SignedData PKCS#7的「簽名資料」部分是EnvelopedData PKCS#7。
5. EnvelopedData PKCS#7是一個包含「加密資料」和「解密金鑰」的容器。 解密金鑰使用接收者的公鑰進行加密。在此特定情況下，接收者是CA;結果。只有CA才能實際解密「加密的資料」。
6. 封裝的PKCS#7的「加密資料」部分是CSR(PKCS#10)。



響應

對SCEP註冊請求的響應為以下三種型別之一：

- **Reject** — 管理員會因以下任何原因拒絕請求：
  金鑰大小無效質詢密碼無效CA無法驗證請求請求要求提供CA未授權的屬性請求由CA不信任的標識簽名
- **掛起**- CA管理員尚未審閱請求。
- **Success** — 接受請求並包含簽名的證書。簽名的證書儲存在一種特殊型別的PKCS#7中，稱為「Degraded Certificates-Only PKCS#7」，這是一種特殊容器，可以容納一個或多個X.509或CRL，但不包含簽名或加密的資料負載。



客戶端重新註冊

在證書到期之前，客戶端需要獲取新證書。續訂和滾動更新之間存在細微的行為差異。當客戶端的ID證書即將到期，並且其到期日期與CA證書的到期日期不同（早於）時，就會發生續訂。當ID證書即將到期，並且其到期日期與CA的證書到期日期相同時，會發生滾動更新。

續約

隨著ID證書到期日期的臨近，SCEP客戶端可能需要獲取新證書。使用者端會產生CSR並完成註冊程式（如先前所定義）。 當前證書用於簽署SignedData PKCS#7，從而向CA證明身份。收到新憑證後，使用者端會立即刪除目前的憑證，並替換為新憑證，新憑證會立即生效。

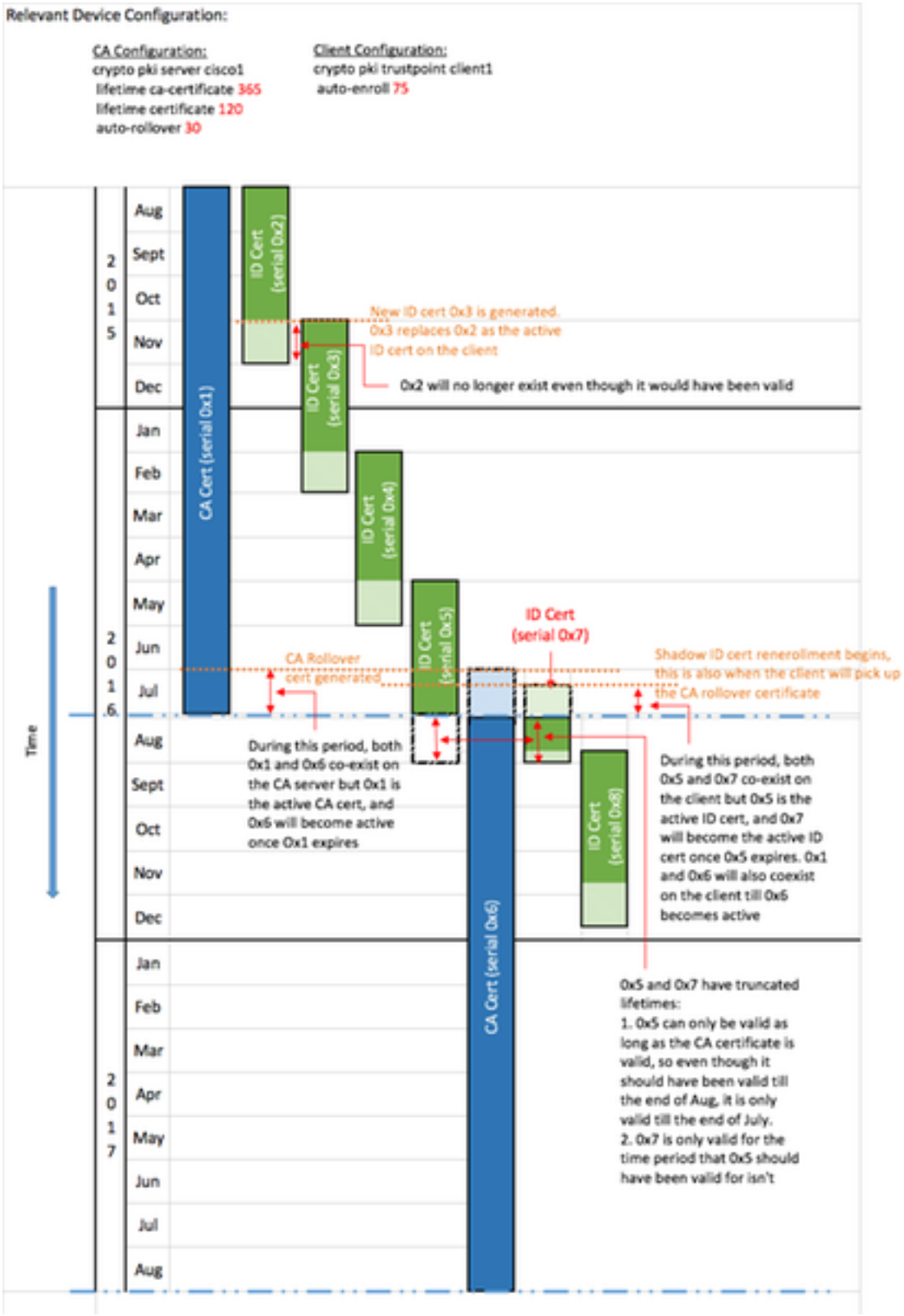
全反

滾動更新是CA證書過期並生成新CA證書的特殊情況。CA產生新的CA證書，該證書在當前的CA證書過期後生效。CA通常會在滾動時間之前的某個時間生成此「影子CA」證書，因為需要為客戶端生成「影子ID」證書。

當SCEP客戶端的ID證書即將到期時，SCEP客戶端將向CA查詢「影子CA」證書。此操作通過**GetNextCACert**操作完成，如下所示：

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

一旦SCEP客戶端具有「影子CA」證書，它將在正常註冊過程後請求「影子ID」證書。CA會使用「影子CA」憑證簽署「影子ID」憑證。與正常的續訂請求不同，返回的「影子ID」證書在CA證書過期（滾動更新）時有效。 因此，客戶端需要保留CA和ID證書的更新前後證書的副本。在CA過期（滾動更新）時，SCEP客戶端刪除當前CA證書和ID證書並用「影子」副本替換它們。



構建基塊

此結構用作SCEP的構建塊。

附註：PKCS#7和PKCS#10不是SCEP特定的。

PKCS#7

PKCS#7是一種允許對資料進行簽名或加密的已定義資料格式。資料格式包括執行加密操作所需的原始資料和相關的後設資料。

簽名信封（簽名資料）

帶簽名的信封是一種傳輸資料的格式，用於確認封裝的資料在傳輸過程中不會通過數位簽章更改。其中包括以下資訊：

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

- 版本號 — 使用SCEP時，使用版本1。
- 使用的摘要演算法清單 — 使用SCEP時，只有一個簽名者，因此只有一個雜湊演算法。
- 帶簽名的實際資料 — 使用SCEP時，這是PKCS#7封裝資料格式（加密信封）。
- 簽名者的證書清單 — 使用SCEP時，這是初始註冊時的自簽名證書或當前證書（如果重新註冊）。
- 簽名者清單和每個簽名者生成的指紋 — 使用SCEP時，只有一個簽名者。

封裝的資料未加密或模糊處理。此格式只是針對被更改的消息提供保護。

封裝資料（封裝資料）

包封資料格式承載加密的資料，並且只能由指定的收件人解密。 其中包括以下資訊：

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

- 版本號 — 對於SCEP，使用版本0。
- 每個收件人和相關加密資料加密金鑰的清單 — 使用SCEP時，只有一個收件人(針對請求：CA伺服器；對於響應：客戶端)。
- 加密的資料 — 使用隨機生成的金鑰（已使用接收者的公鑰加密）進行加密。

PKCS#10

PKCS#10說明CSR的格式。CSR包含使用者端要求包含在其憑證中的資訊：

- 使用者名稱
- 公鑰的副本
- 質詢密碼（可選）

- 需要的任何證書擴展，例如：
  金鑰用法(KU)延伸金鑰使用(EKU)使用者替代名稱(SAN)通用主體名稱(UPN)
- 請求的指紋

以下是CSR的範例：

```
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
```

相關資訊

- SCEP IETF草案
- 使用CLI配置指南的傳統SCEP
- 為BYOD配置SCEP支援

附錄

SCEP請求

請求消息格式

請求採用以下格式的HTTP GET傳送：

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

其中：

- **CGI-path**取決於伺服器，指向處理SCEP請求的通用網關介面(CGI)程式： Cisco IOS® CA使用空路徑字串。Microsoft CA使用**/certsrv/mscep/mscep.dll**，它指向MSCEP/網路裝置註冊服務(NDES)IIS服務。
- **操**作標識執行的操作。
- **消息**攜帶該操作的附加資料（並且如果不需要實際資料，則該消息可以為空）。

使用GET方法時，消息部分可以是純文字檔案，也可以是轉換為Base64的可分辨編碼規則(DER)編碼的PKCS#7。如果支援POST方法，則使用GET的Base64編碼傳送的內容可能會改為使用POST以二進位制格式傳送。

示意性檢視

操作的可能值及其關聯的**消息**值：

- **operation** = `PKIOperation`: **消息**是基於**PKCS#**7並使用DER和Base64編碼的SCEP pkiMessage結構。**pkiMessage**結構可以是以下型別： **PKCSReq**:PKCS#10 CSR**GetCertInitial**:正在輪詢CSR授予狀態**GetCert**或**GetCRL**:證書或CRL檢索
- **operation** = **GetCACert**、**GetNextCACert**或（可選）**GetCACaps**: **消**息可以省略，也可以設定為標識CA的名稱。

SCEP響應

響應消息格式

SCEP響應作為標準HTTP內容返回，其**Content-Type**取決於原始請求和返回的資料型別。DER內容以二進位制形式返回（對於請求不以Base64形式返回）。PKCS#7內容可能包含加密/已簽名的信封資料，也可能不包含這些資料；如果沒有（僅包含一組證書），則將其稱為PKCS#7。

內容型別

Content-Type的可能值：

application/x-pki-message:

- 響應PKIOperation**操**作，**pkiMessage**型別：**PKCSReq**、**GetCertInitial**、**GetCert**或**GetCRL**
- 響應正文是**pkiMessage**型別：**CertRep**

application/x-x509-ca-cert:

- 響應GetCACert**操**作
- 響應正文是DER編碼的X.509 CA證書

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

- 響應GetCACert**操**作
- 響應正文是包含CA和RA證書的DER編碼簡並PKCS#7

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

- 響應GetNextCACert操作
- 響應正文是以下型別的pkiMessage的變體：CertRep

pkiMessage結構

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 EnvelopedData(稱為pkcsPKIEnvelope;可選，已加密郵件收件人)
  messageData(CSR、cert、CRL、...)
- 具有authenticatedAttributes的簽名者信息：
  transactionID、messageType、senderNoncepkiStatus、recipientNonce（僅限響應）failInfo（僅響應+故障）

SCEP messageType

- 請求：
  PKCSReq(19):PKCS#10 CSRGetCertInitial(20):證書註冊輪詢GetCert(21):證書檢索
  GetCRL(22):CRL檢索
- 響應：
  CertRep(3):對證書或CRL請求的響應

SCEP pkiStatus

- 成功(0):請求已授權（pkcsPKIEnvelope中的響應）
- 故障(2):請求被拒絕（failInfo屬性中的詳細資訊）
- 待定(3):請求等待手動批准