Simple Certificate Enrollment Protocol 개요

목차

소개

이 문서에서는 등록 및 기타 PKI(Public Key Infrastructure) 작업에 사용되는 프로토콜인 SCEP(Simple Certificate Enrollment Protocol)에 대해 설명합니다.

배경 정보

SCEP는 원래 Cisco에서 개발되었으며 IETF(Internet Engineering Task Force) 초안에 문서화되어 있습니다.

주요 특징은 다음과 같습니다.

- HTTP(GET 메서드,POST 방법에 대한 선택적 지원)
- RSA 기반 암호화 만 지원
- PKCS#10을 인증서 요청 형식으로 사용
- 암호화 서명/암호화 메시지를 전달하기 위해 PKCS#7을 사용합니다.
- 요청자의 정기적인 폴링을 통해 서버에서 비동기 권한 부여를 지원합니다.
- 제한된 CRL(Certificate Revocation List) 검색 지원(확장성으로 인해 CDP(CRL Distribution Point) 쿼리를 통해 선호하는 방법)
- 온라인 인증서 해지를 지원하지 않음(다른 방법을 통해 오프라인으로 수행해야 함)
- CSR(Certificate Signing Request) 내에서 **챌린지 비밀번호** 필드를 사용해야 합니다. 이 필드는 서버와 요청자 간에만 공유되어야 합니다.

SCEP의 등록 및 사용량은 일반적으로 다음과 같습니다.

1. CA(Certificate Authority) 인증서의 복사본을 가져와서 검증합니다.
2. CSR을 생성하고 CA에 안전하게 전송합니다.
3. 인증서가 서명되었는지 확인하기 위해 SCEP 서버를 폴링합니다.
4. 현재 인증서가 만료되기 전에 새 인증서를 얻으려면 필요에 따라 다시 등록합니다.
5. 필요에 따라 CRL을 검색합니다.

CA 인증

SCEP는 CSR에 대한 메시지 교환을 보호하기 위해 CA 인증서를 사용합니다.따라서 CA 인증서의 사본을 가져와야 합니다.GetCACert **작업**이 사용됩니다.

요청

요청이 HTTP GET 요청으로 전송됩니다.요청에 대한 패킷 캡처는 다음과 유사합니다.

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

응답

응답은 단순히 이진 인코딩 CA 인증서(X.509)입니다. 클라이언트는 핑거프린트/해시의 검사를 통해 CA 인증서가 신뢰되는지 확인해야 합니다.이는 대역외 방법(시스템 관리자에게 전화 통화하거나 신뢰 지점 내에서 핑거프린트의 사전 컨피그레이션)을 통해 수행해야 합니다.

클라이언트 등록

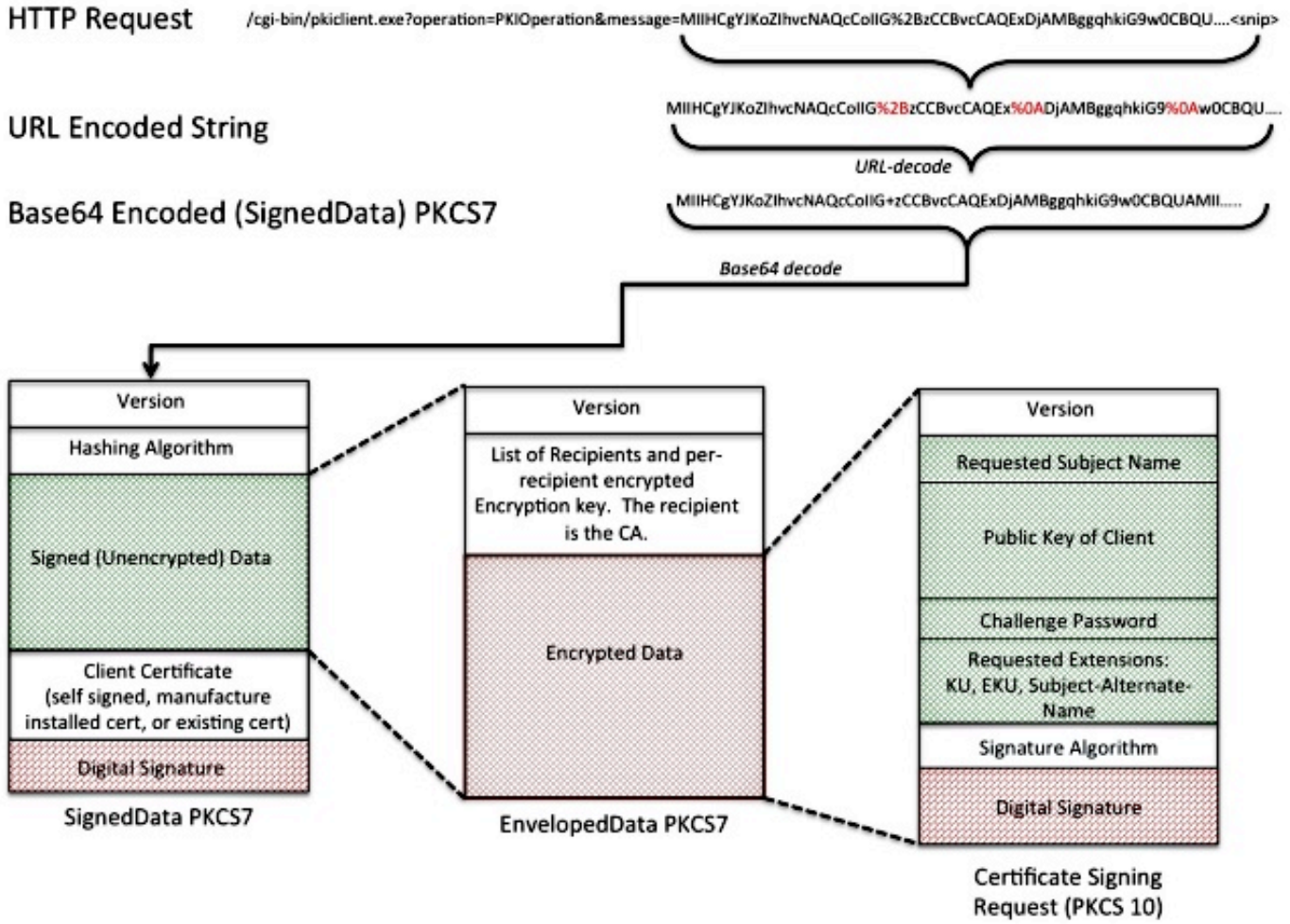
요청

등록 요청이 HTTP GET 요청으로 전송됩니다. 요청에 대한 패킷 캡처는 다음과 같습니다.

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

1. "message=" 뒤의 텍스트는 GET 요청 문자열에서 추출되는 URL 인코딩 문자열입니다.
2. 그러면 URL이 ASCII 텍스트 문자열로 디코딩됩니다.해당 텍스트 문자열은 Base64로 인코딩

된 SignedData PKCS#7입니다.
3. SignedData PKCS#7은 클라이언트가 이러한 인증서 중 하나를 사용하여 서명합니다.클라이언트가 전송했으며 전송 중에 변경되지 않았음을 입증하는 데 사용됩니다.
   자체 서명 인증서(초기 등록 시 사용)제조업체 설치 인증서(MIC)곧 만료되는 현재 인증(재등록)
4. SignedData PKCS#7의 "Signed Data" 부분은 EnvelopedData PKCS#7입니다.
5. EnvelopedData PKCS#7은 "Encrypted Data" 및 "암호 해독 키"를 포함하는 컨테이너입니다.
   암호 해독 키는 수신자의 공개 키로 암호화됩니다.이 경우 수신자는 CA입니다.있습니다CA만 실제로 "Encrypted Data"를 해독할 수 있습니다.
6. Enveloped PKCS#7의 "Encrypted Data" 부분은 CSR(PKCS#10)입니다.

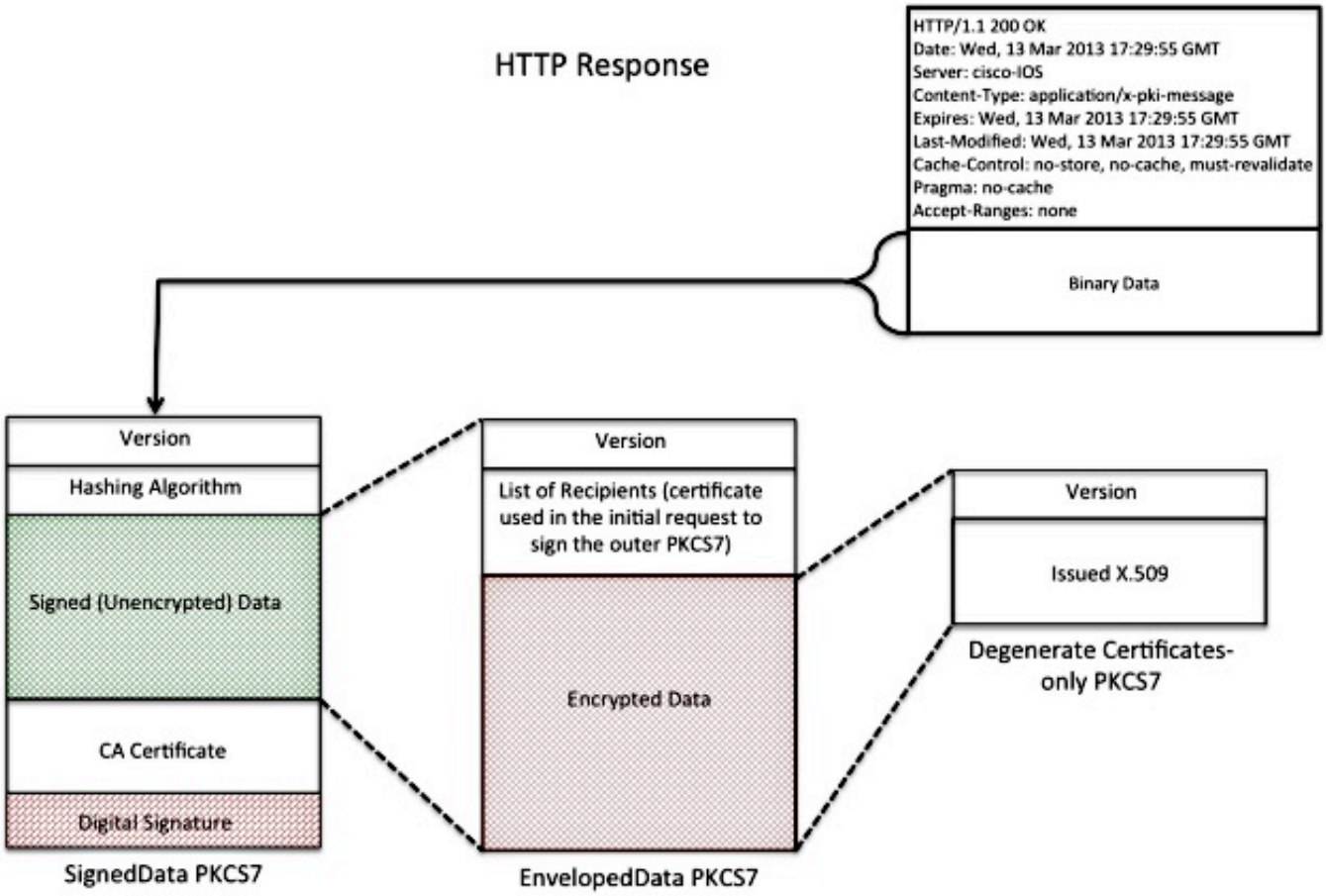


응답

SCEP 등록 요청에 대한 응답은 다음 세 가지 유형 중 하나입니다.

- **거부** - 다음과 같은 여러 가지 이유로 관리자가 요청을 거부합니다.
  키 크기가 잘못되었습니다.잘못된 챌린지 비밀번호CA가 요청을 검증할 수 없습니다.요청에서 CA가 인증하지 않은 속성을 요청했습니다.요청이 CA가 신뢰하지 않는 ID에 의해 서명되었습니다.
- **Pending** - CA 관리자가 요청을 아직 검토하지 않았습니다.
- **성공** - 요청이 수락되고 서명된 인증서가 포함됩니다.서명된 인증서는 PKCS#7의 특수 유형인 "Degenerate Certificates-Only PKCS#7"에 저장됩니다. 이 특수 컨테이너에서는 하나 이상의 X.509 또는 CRL을 보관할 수 있지만 서명 또는 암호화된 데이터 페이로드를 포함하지 않습니

다.



클라이언트 재등록

인증서가 만료되기 전에 클라이언트는 새 인증서를 가져와야 합니다.갱신과 롤오버 사이에는 약간의 동작 차이가 있습니다.갱신은 클라이언트의 ID 인증서가 만료에 가까워지고 만료 날짜가 CA 인증서의 만료 날짜와 같거나 이전 날짜가 아닌 경우 발생합니다.ID 인증서가 만료에 가까워지고 만료 날짜가 CA의 인증서 만료 날짜와 같을 때 롤오버가 발생합니다.

갱신

ID 인증서의 만료 날짜가 다가옴에 따라 SCEP 클라이언트는 새 인증서를 얻을 수 있습니다.클라이언트는 CSR을 생성하고 이전에 정의한 등록 프로세스를 거칩니다. 현재 인증서는 SignedData PKCS#7에 서명하기 위해 사용되며, 이 경우 CA에 ID를 검증합니다.새 인증서를 받으면 클라이언트는 즉시 현재 인증서를 삭제하고 해당 인증서가 즉시 유효성 검사가 시작되는 새 인증서로 대체합니다.

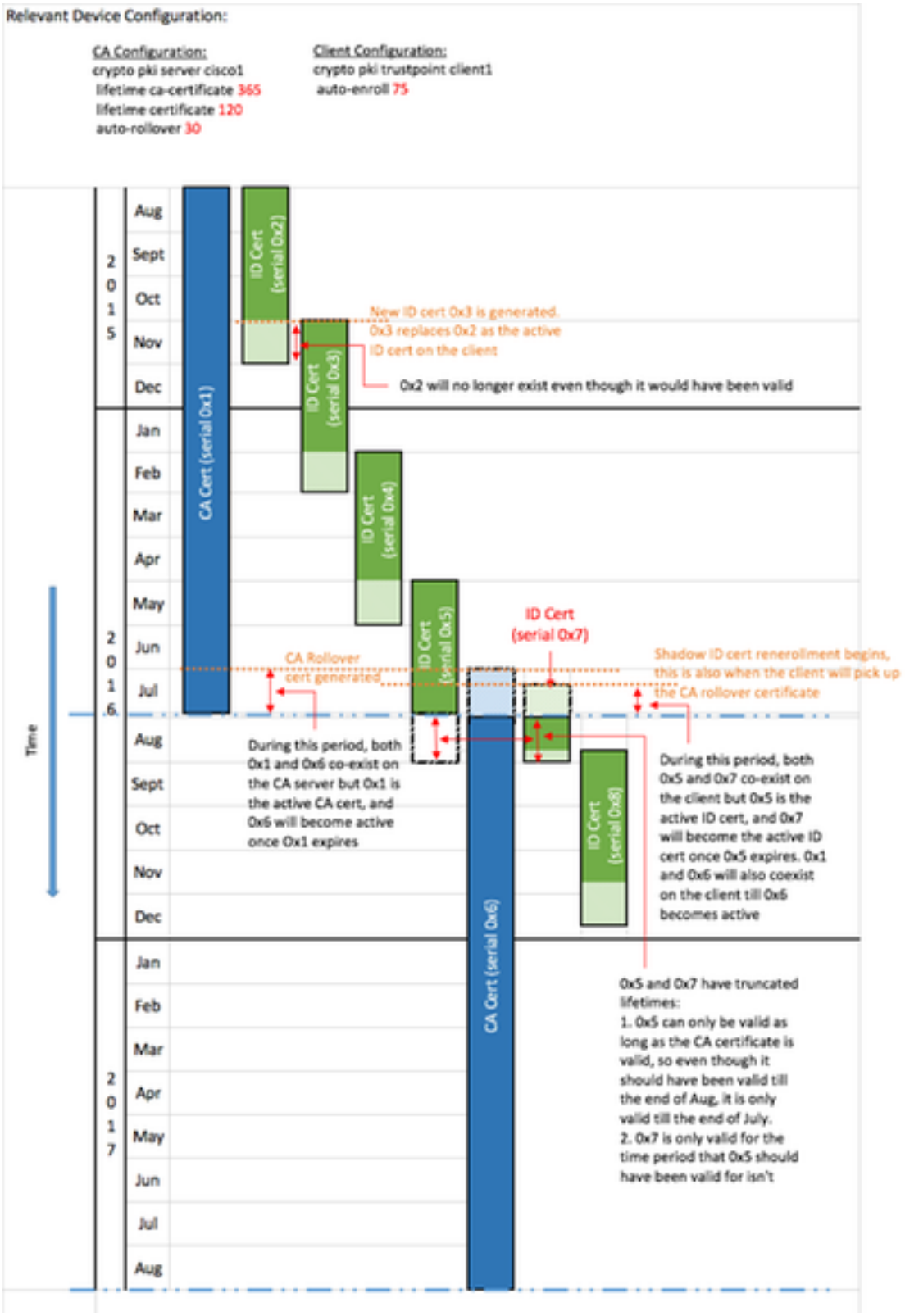
롤오버

롤오버는 CA 인증서가 만료되고 새 CA 인증서가 생성되는 특수한 경우입니다.CA는 현재 CA 인증서가 만료되면 유효한 새 CA 인증서를 생성합니다.일반적으로 CA는 클라이언트에 대한 "Shadow ID" 인증서를 생성하기 위해 필요하기 때문에 롤오버 시간 전에 이 "Shadow CA" 인증서를 생성합니다.

SCEP 클라이언트의 ID 인증서가 만료될 때 SCEP 클라이언트는 CA에 "Shadow CA" 인증서를 쿼리합니다.이 작업은 다음과 같이 **GetNextCACert** 작업을 통해 수행됩니다.

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

SCEP 클라이언트에 "Shadow CA" 인증서가 있으면 일반 등록 절차 후에 "Shadow ID" 인증서를 요청합니다.CA는 "Shadow CA" 인증서로 "Shadow ID" 인증서에 서명합니다.일반적인 갱신 요청과 달리, 반환되는 "Shadow ID" 인증서는 CA 인증서 만료(롤오버) 시 유효하게 됩니다. 따라서 클라이언트는 CA와 ID 인증서 모두에 대해 사전 및 사후 롤오버 인증서의 사본을 유지해야 합니다.CA 만료(롤오버) 시 SCEP 클라이언트는 현재 CA 인증서 및 ID 인증서를 삭제하고 "Shadow" 복사본으로 대체합니다.



빌딩 블록

이 구조는 SCEP의 구성 요소로 사용됩니다.

참고:PKCS#7 및 PKCS#10은 SCEP에 한정되지 않습니다.

PKCS#7

PKCS#7은 데이터를 서명 또는 암호화할 수 있는 정의된 데이터 형식입니다.데이터 형식에는 암호화 작업을 수행하는 데 필요한 원본 데이터 및 관련 메타데이터가 포함됩니다.

서명된 봉투(SignedData)

서명된 봉투는 데이터를 전송하고 캡슐화된 데이터가 디지털 서명을 통해 전송 중에 변경되지 않음을 확인하는 형식입니다.여기에는 다음 정보가 포함됩니다.

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

- 버전 번호 - SCEP와 함께 버전 1이 사용되었습니다.
- 사용된 다이제스트 알고리즘 목록 - SCEP에는 서명자가 하나만 있으므로 해싱 알고리즘이 하나만 사용됩니다.
- 서명된 실제 데이터 - SCEP를 사용하는 경우 PKCS#7 Enveloped-data 형식(Encrypted Envelope)입니다.
- 서명자의 인증서 목록 - SCEP를 사용하면 초기 등록 시 자체 서명된 인증서나 재등록 시 현재 인증서입니다.
- 서명자 목록 및 각 서명자가 생성한 핑거프린트. SCEP를 사용하는 경우 서명자가 하나만 있습니다.

캡슐화된 데이터는 암호화되지 않거나 애매합니다.이 형식은 변경된 메시지에 대한 보호를 제공합니다.

봉투 데이터(EnvelopedData)

Enveloped Data 형식은 암호화된 데이터를 전송하며, 지정된 수신자만 해독할 수 있습니다. 여기에는 다음 정보가 포함됩니다.

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

- 버전 번호 - SCEP에서는 버전 0이 사용됩니다.
- 각 수신자 목록 및 관련 암호화된 데이터 암호화 키 - SCEP를 사용하는 경우 수신자가 하나만 있습니다(요청의 경우:CA 서버,응답:클라이언트).
- 암호화된 데이터 - 임의로 생성된 키(수신자의 공개 키로 암호화됨)로 암호화됩니다.

PKCS#10

PKCS#10은 CSR의 형식을 설명합니다.CSR에는 클라이언트 요청이 해당 인증서에 포함되는 정보가 포함됩니다.

- 주체 이름
- 공개 키 사본

- 챌린지 비밀번호(선택 사항)
- 필요한 모든 인증서 확장(예:
  키 사용(KU)확장 키 사용(EKU)SAN(주체 대체 이름)UPN(Universal Principal Name)
- 요청의 지문

다음은 CSR의 예입니다.

```
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
```

관련 정보

- SCEP IETF 초안
- CLI 컨피그레이션 가이드를 사용하는 레거시 SCEP
- BYOD에 대한 SCEP 지원 구성

부록

SCEP 요청

요청 메시지 형식

요청은 양식의 HTTP GET을 사용하여 전송됩니다.

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

위치:

- **CGI-path**는 서버에 종속되며 SCEP 요청을 처리하는 CGI(Common Gateway Interface) 프로그램을 가리킵니다. Cisco IOS® CA는 빈 경로 문자열을 사용합니다.Microsoft CA는 **/certsrv/mscep/mscep.dll을** 사용하며, MSCEP/NDES(Network Device Enrollment Service) IIS 서비스를 가리킵니다.
- **작업**은 수행되는 작업을 식별합니다.
- **메시지**는 해당 작업에 대한 추가 데이터를 전달합니다. 실제 데이터가 필요하지 않은 경우 비어 있을 수 있습니다.

GET 메서드를 사용하면 **메시지** 파트가 일반 텍스트 또는 DER(Distinguished Encoding Rules) 인코딩 PKCS#7이 Base64로 변환됩니다. POST 메서드가 지원되는 경우 GET을 사용하여 Base64 인코딩으로 전송되는 콘텐츠가 대신 POST를 사용하여 이진 형식으로 전송될 수 있습니다.

도식 뷰

작업 및 관련 **메시지** 값에 사용할 수 있는 값

- **작업** = `PKIOperation`: **메시지**PKCS#7을 기반으로 하고 DER 및 Base64로 인코딩된 SCEP pkiMessage 구조입니다.pkiMessage **구조**는 다음 유형이 될 수 있습니다. **PKCSReq**:PKCS#10 CSR**GetCertInitial**:CSR 부여 상태에 대한 폴링**GetCert** 또는 **GetCRL**:인증서 또는 CRL 검색
- **operation** = **GetCACert**, **GetNextCACert** 또는 (선택 사항) **GetCACaps**: **메시지**를 생략하거나 CA를 식별하는 이름으로 설정할 수 있습니다.

SCEP 응답

응답 메시지 형식

SCEP 응답은 표준 HTTP 콘텐츠로 반환되며 원래 요청 및 반환된 데이터 유형에 따라 달라지는 **Content-Type**이 사용됩니다.DER 콘텐츠는 요청에 대한 Base64가 아닌 이진으로 반환됩니다 .PKCS#7 콘텐츠에는 암호화된/서명된 enveloped 데이터가 포함되거나 포함되지 않을 수 있습니다 .인증서 집합이 포함되지 않은 경우(인증서 집합만 포함), 이를 **dergenerate** PKCS#7**이라고** 합니다.

콘텐츠 형식

콘텐츠 형식에 사용할 수 있는 값:

application/x-pki-message:

- pkiMessage 유형을 사용하여 **PKIOperation** 작업**에** 응답합니다.**PKCSReq, GetCertInitial, GetCert 또는 GetCRL**
- 응답 본문은 **pkiMessage** 유형:**인증서 담당자**

application/x-x509-ca-cert:

- GetCACert 작업에 대한 **응답으로**
- 응답 본문은 DER로 인코딩된 X.509 CA 인증서입니다.

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

- GetCACert 작업에 대한 **응답으로**
- 응답 본문은 CA 및 RA 인증서를 포함하는 DER로 인코딩된 PKCS#7입니다.

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

- GetNextCACert **작업**에 **대한** 응답으로
- 응답 본문은 pkiMessage의 유형의 변형입니다.**인증서 담당자**

pkiMessage 구조

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 **서명데이터**
- PKCS#7 EnvelopedData(pkcsPKIEnvelope**라고 함**;선택 사항, 메시지 수신자에게 암호화 **messageData**(CSR, 인증서, CRL, ...)
- **인증된 특성이** 있는 **SignerInfo**: **transactionID**, **messageType**, senderNonce**pkiStatus**, **recipientNonce**(응답만 해당)**failInfo**(응답 + 실패만)

SCEP 메시지 유형

- 요청: **PKCSReq**(19):PKCS#10 CSR**GetCertInitial**(20):인증서 등록 폴링**GetCert**(21):인증서 검색 **GetCRL**(22):CRL 검색
- 응답: **CertRep**(3):인증서 또는 CRL 요청에 대한 응답

SCEP pkiStatus

- **성공**(0):요청 부여됨(pkcsPKIEnvelope의 응답)
- **실패**(2):request rejected(failInfo 특성의 세부사항)
- **보류** 중(3):수동 승인 요청