نظرة عامة على بروتوكول تسجيل الشهادة البسيط

المحتويات

المقدمة

يصف هذا المستند بروتوكول تسجيل الشهادة البسيط (SCEP)، وهو بروتوكول يستخدم للتسجيل وعمليات البنية الأساسية للمفاتيح العام (PKI) الأخرى.

معلومات أساسية

تم تطوير بروتوكول SCEP في الأصل بواسطة Cisco، ويتم توثيقه في مسودة مشروع

فرقة عمل هندسة الإنترنت (IETF).

وخصائصه الرئيسية هي:

- نموذج الطلب/الاستجابة المستند إلى HTTP (أسلوب GET؛ الدعم الاختياري لأسلوب POST)
- يدعم فقط التشفير المستند إلى RSA
- يستخدم PKCS#10 كتنسيق طلب الشهادة
- يستخدم PKCS#7 من أجل نقل رسائل مشفرة وموقعة/مشفرة
- يدعم منح غير متزامن بواسطة الخادم، مع فحص دوري بواسطة الطالب
- لديه دعم إسترداد محدود لقائمة إبطال الشهادات (CRL) (الطريقة المفضلة هي من خلال استعلام نقطة توزيع CRL (CDP)، لأسباب تتعلق بقابلية التوسع)
- لا يعتمد إلغاء الشهادة عبر الإنترنت (يجب أن يتم دون اتصال من خلال وسائل أخرى)
- يتطلب إستخدام حقل **تحدي كلمة المرور** داخل طلب توقيع الشهادة (CSR)، والذي يجب مشاركته فقط بين الخادم والطالب

يتبع تسجيل SCEP واستخدامه بشكل عام تدفق العمل هذا:

1. الحصول على نسخة من شهادة المرجع المصدق والتصديق عليها.
2. قم بإنشاء CSR وإرساله بأمان إلى CA.
3. قم باستطلاع خادم SCEP للتحقق مما إذا كانت الشهادة موقعة أم لا.
4. قم بإعادة التسجيل حسب الحاجة للحصول على شهادة جديدة قبل انتهاء صلاحية الشهادة الحالية.
5. قم باسترداد قائمة التحكم في الوصول (CRL) حسب الضرورة.

مصادقة CA

يستخدم SCEP شهادة CA لتأمين تبادل الرسائل ل CSR. وتنتيجة لذلك، من الضروري الحصول على نسخة من شهادة المرجع المصدق. يتم إستخدام عملية **GetCACert**.

طلب

يتم إرسال الطلب كطلب HTTP GET. يبدو التقاط حزمة للطلب مماثلا لهذا:

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

إستجابة

الاستجابة هي بسلطة شهادة CA المرمزة ثنائيا (X.509). يحتاج العميل إلى التحقق من أن شهادة CA موثوق بها من خلال فحص بصمة الإصبع/التجزئة. ويجب أن يتم ذلك من خلال طريقة خارج النطاق (مكالمة هاتفية لمسؤول النظام أو تهيئة مسبقة لبصمة الإصبع كجزء من TrustPoint).

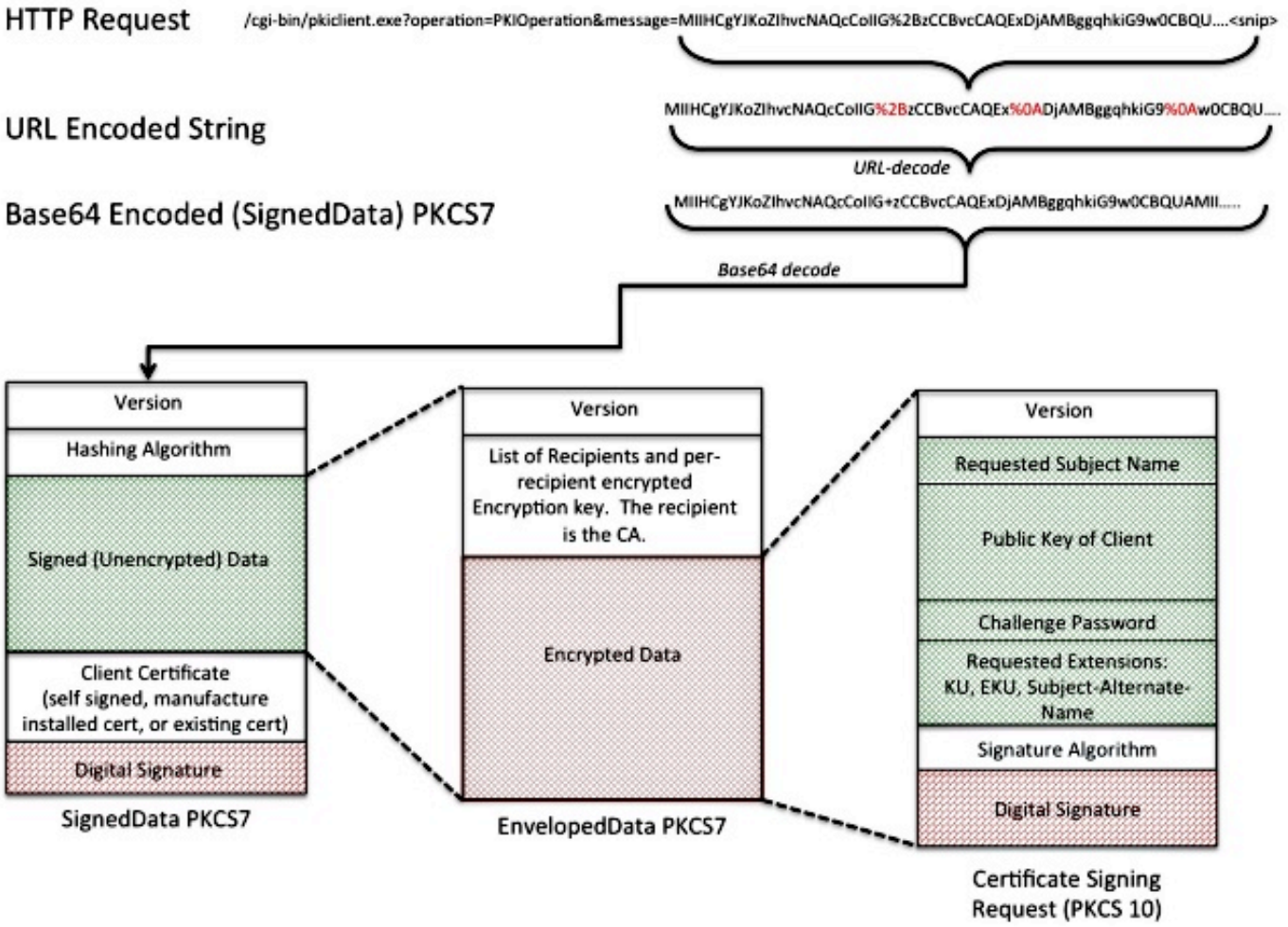
تسجيل العميل

طلب

تم إرسال طلب التسجيل كطلب HTTP GET. يبدو التقاط حزمة للطلب مماثلا لهذا:

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

1. النص بعد "message=" وه سلسلة URL مرمزة، والتي يتم إستخراجها من سلسلة طلب GET.
2. يتم بعد ذلك فك ترميز النص إلى سلسلة نصية ASCII. تلك السلسلة النصية هي PKCS#7 مرمز إلى Base64.
3. يتم توقيع SignedData PKCS#7 من قبل العميل مع إحدى هذه الشهادات، ويتم إستخدامها لإثبات أن العميل أرسلها وأنه لم يتم تغييرها أثناء النقل:
شهادة موقعة ذاتيا (تستخدم عند التسجيل الأولي)شهادة مثبتة من جهة مصنعة (إعادة التسجيل)شهادة حالية تنتهي صلاحيتها قريبا (MIC)
4. جزء "البيانات الموقعة" من SignedData PKCS#7 وه EnvelopeData PKCS#7.
5. EnvelopeData PKCS#7 هي حاوية تحتوي على "بيانات مشفرة"و"مفتاح فك التشفير". يتم تشفير مفتاح فك التشفير باستخدام المفتاح العام الخاص بالمستلم. وفي هذه الحالة بالذات، يكون المتلقي وه المرجع المصدق؛ ونتيجة لذلك. يمكن فقط ل CA فك تشفير "البيانات المشفرة".
6. جزء "البيانات المشفرة" من PKCS#7 المغلف وه CSR (PKCS#10).



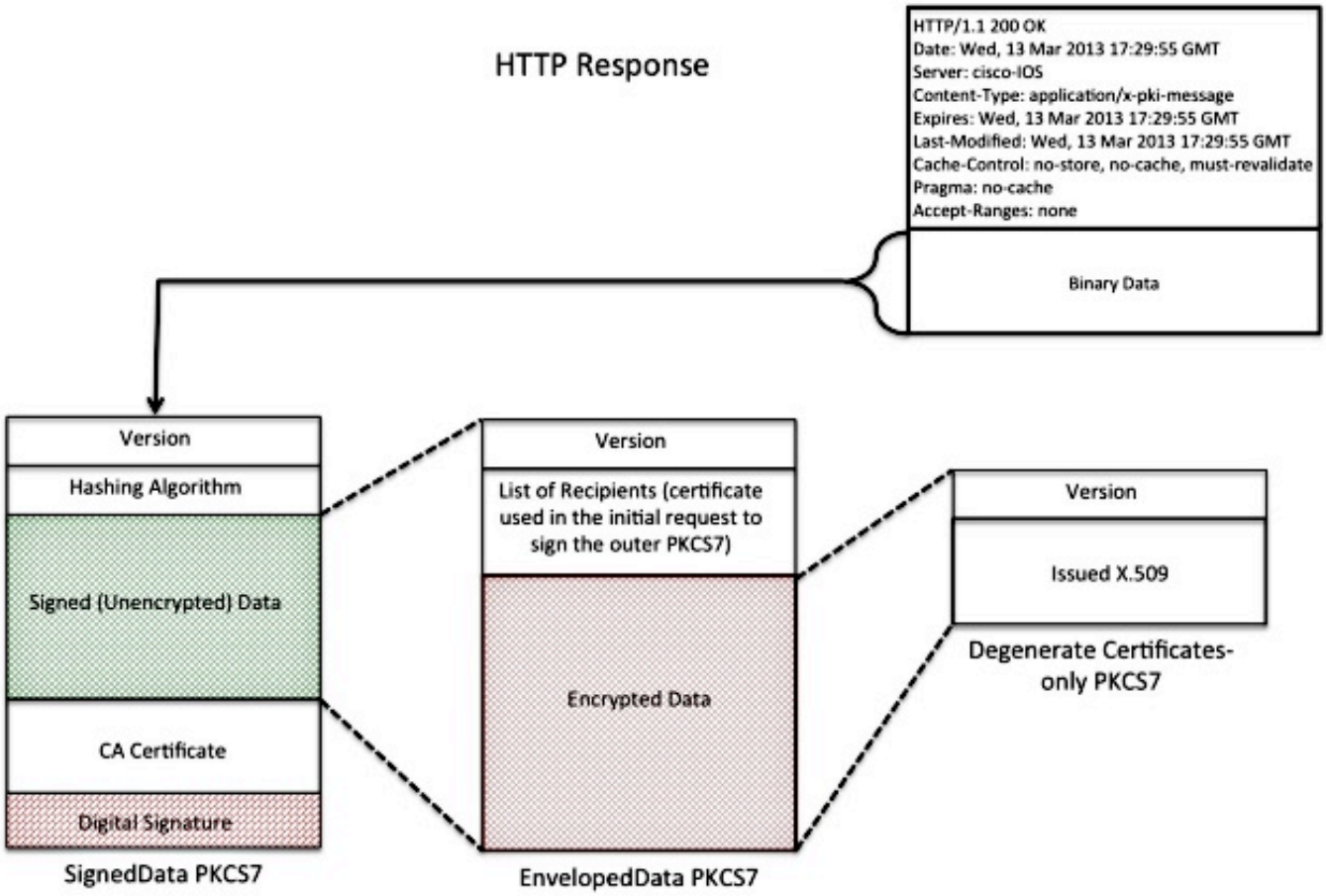
إستجابة

تعد الاستجابة لطلب تسجيل SCEP أحد الأنواع الثلاثة التالية:

- **رفض** - رفض المسؤول الطلب لأي عدد من الأسباب، مثل:
حجم مفتاح غير صالحكلمة مرور التحدي غير صالحةتعذر على المرجع المصدق التحقق

من صحة الطلبطلب الحصول على سمات لم تخولها المرجع المصدقتم توقيع الطلب بواسطة هويه ال يثق بها المرجع المصدق

- **معلق** - لم يقم مسؤول CA بمراجعة الطلب بعد.
- **نجاح** - تم قبول الطلب وتضمين الشهادة الموقعة. يتم الاحتفاظ بالشهادة الموقعة ضمن نوع خاص من PKCS#7 يسمى "Degenerate Certificates-Only PKCS#7"، وهو عبارة عن حاوية خاصة يمكن أن تحتوي على واحد أو أكثر من X.509 أو CRLs، ولكنها لا تحتوي على حمولة بيانات موقعة أو مشفرة.



إعادة تسجيل العميل

قبل انتهاء صلاحية الشهادة، يحتاج العميل إلى الحصول على شهادة جديدة. هناك فارق سلوكي طفيف بين التجديد وإعادة التوجيه. يحدث التجديد عندما تقترب شهادة مُعرف العميل من انتهاء الصلاحية، ويكون تاريخ انتهاء الصلاحية غير مماثل (أقدم من) لتاريخ انتهاء صلاحية شهادة المرجع المصدق. يحدث التبديل عندما تقترب شهادة المعرف من الانتهاء، ويكون تاريخ انتهاء صلاحيتها هو نفس تاريخ انتهاء صلاحية شهادة CA.

تجديد

مع اقتراب تاريخ انتهاء صلاحية شهادة المعرف، قد يرغب عميل SCEP في الحصول على شهادة جديدة. يقوم العميل بإنشاء CSR ويمر بعملية التسجيل (كما هو محدد مسبقا). يتم إستخدام الشهادة الحالية لتوقيع SignedData PKCS#7، والتي تثبت بدورها الهوية إلى CA. عند إستلام الشهادة الجديدة، يقوم العميل فورا بحذف الشهادة الحالية ويستبدلها بالشهادة الجديدة التي تبدأ صلاحيتها فورا.

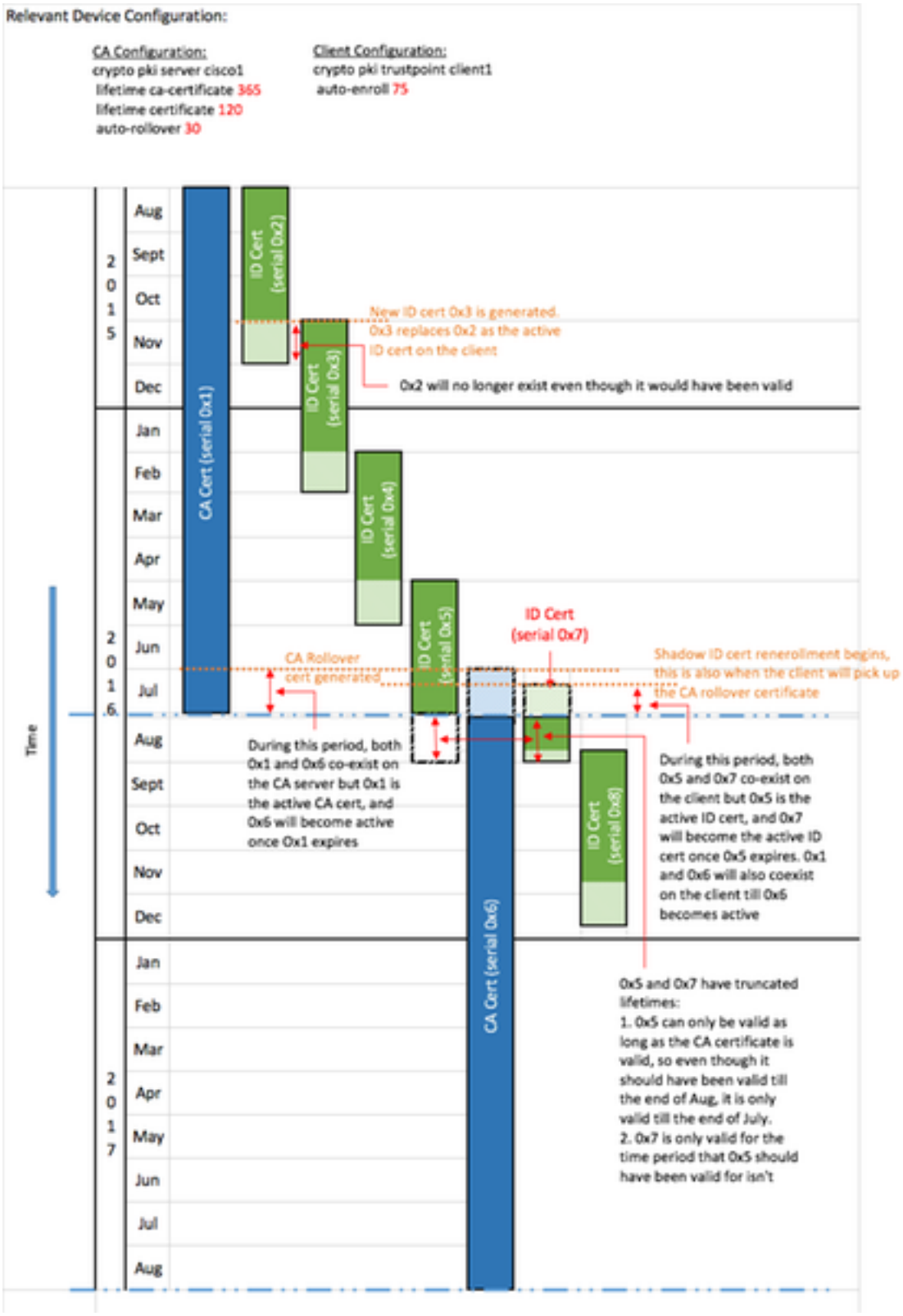
تمرير

التمرير وه حالة خاصة تنتهي فيها صلاحية شهادة CA ويتم إنشاء شهادة CA جديدة. يقوم المرجع المصدق بإنشاء شهادة مرجع مصدق جديدة تصبح صالحة بمجرد انتهاء صلاحية شهادة المرجع المصدق الحالية. عادة ما يقوم المرجع المصدق بإنشاء شهادة "Shadow CA" هذه في بعض الوقت قبل وقت إعادة التوجيه، لأنها مطلوبة لإنشاء شهادات "Shadow ID" للعملاء.

عندما تقترب شهادة معرف عميل SCEP من الانتهاء، يستعلم عميل SCEP عن المرجع المصدق لشهادة "Shadow CA". ويتم القيام بذلك باستخدام عملية **GetNextCACert** كما هو موضح هنا:

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

بمجرد حصول عميل SCEP على شهادة "Shadow CA"، فإنه يطلب شهادة "Shadow ID" بعد إجراء التسجيل العادي. يوقع المرجع المصدق شهادة "معرف الظل" بشهادة "مرجع الظل". بخلاف طلب التجديد العادي، تصبح الشهادة "معرف الظل" التي يتم إرجاعها صالحة في وقت انتهاء صلاحية شهادة CA (إعادة توجيه). ونتيجة لذلك، يحتاج العميل إلى الاحتفاظ بنسخة من شهادات المعرف الحالية وشهادة المرجع المصدق وشهادة CA (إعادة توجيه)، يحذف عميل SCEP شهادة المعرف الحالية وشهادة CA لكل من هذه الشهادات قبل النقل ومعه بعد انتهاء صلاحية شهادة CA (إعادة توجيه)، يحذف عميل SCEP شهادة المعرف الحالية وشهادة CA ويستبدلهما بنسخ "الظل".



كتل البناء

يتم إستخدام هذا الهيكل كتل إنشاء SCEP.

ملاحظة: PKCS#7 و PKCS#10 ليست خاصة ب SCEP.

PKCS#7

PKCS#7 وه تنسيق بيانات معرف يسمح بتوقيع البيانات أو تشفيرها. يتضمن تنسيق البيانات البيانات الأصلية وبيانات التعريف المقترنة الضرورية لتنفيذ عملية التشفير.

المظروف الموقع (SignedData)

المظروف الموقع وه تنسيق يحمل البيانات ويؤكد أن البيانات المغلفة ال يتم تغييرها أثناء النقل عبر التوقيعات الرقمية. وتتضمن هذه المعلومات:

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

- رقم الإصدار - مع إستخدام SCEP، الإصدار 1.
- قائمة خوارزميات الهضم المستخدمة - مع SCEP، يوجد موقع واحد فقط وبالتالي خوارزمية تجزئة واحدة.
- البيانات الفعلية الموقعة - باستخدام SCEP، هذا وه تنسيق PKCS#7 للبيانات المغلفة (المظروف المشفر).
- قائمة شهادات الموقعين - باستخدام SCEP، هذه هي شهادة موقعة ذاتيا في التسجيل الأولي أو الشهادة الحالية إذا قمت بإعادة التسجيل.
- قائمة الموقعين وبصمة الأصابع التي تم توليدها من قبل كل موقع - مع SCEP، يوجد موقع واحد فقط.

البيانات المضمنة غير مشفرة أو مبهمة. يوفر هذا التنسيق ببساطة الحماية ضد الرسالة التي يتم تغييرها.

بيانات مغلفة (مغلفData)

يحمل تنسيق البيانات المغلف بيانات مشفرة والتي يمكن فك تشفيرها إلا بواسطة المستلم (المستلمين) المحدد. وتتضمن هذه المعلومات:

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

- رقم الإصدار - باستخدام SCEP، يتم إستخدام الإصدار 0.
- قائمة لكل من المستلمين ومفاتيح تشفير البيانات المشفر المرتبط به - مع SCEP، يوجد مستلم واحد فقط (للطلبات: خادم CA؛ للاستجابات: العميل).
- البيانات المشفرة - يتم تشفير هذه البيانات باستخدام مفتاح تم إنشاؤه بشكل عشوائي (تم تشفيره باستخدام المفتاح العام الخاص بالمستلم).

PKCS#10

يصف PKCS#10 تنسيق CSR. تحتوي CSR على المعلومات التي يطلبها العملاء لتضمين شهاداتهم:

- اسم الموضوع
- نسخة من المفتاح العام
- كلمة مرور تحدي (إختيارية)
- أي ملحقات للشهادات مطلوبة، مثل:
  إستخدام المفتاح (KU)إستخدام المفتاح الموسع (EKU)الاسم البديل للموضوع (SAN)اسم أساسي عام (UPN)
- بصمة الإصبع للطلب

فيما يلي مثال على CSR:

```
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
```

معلومات ذات صلة

- بروتوكول SCEP IETF Draft
- SCEP القديمي باستخدام دليل تكوين واجهة سطر الأوامر
- تكوين دعم SCEP ل BYOD

الملحق

طلبات SCEP

تنسيق رسالة الطلب

يتم إرسال الطلبات مع HTTP GET من النموذج :

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

أين:

- يعتمد **مسار CGI** على الخادم ويشير إلى برنامج الواجهة المشتركة للعبارة (CGI) الذي يعالج طلبات SCEP: يستخدم Cisco IOS® CA سلسلة مسار فارغة.يستخدم Microsoft CA **/certsrv/mscep/mscep.dll**، مما يشير إلى خدمة IIS لخدمة تسجيل أجهزة الشبكة/MSCEP (NDES).
- تحدد **العملية** العملية التي يتم تنفيذها.
- تحمل **الرسالة** بيانات إضافية لتلك العملية (ويمكن أن تكون فارغة إذا لم تكن هناك حاجة إلى بيانات فعلية).

باستخدام أسلوب GET، فإن **جزء الرسالة** إما نص عادي، أو قواعد الترميز المميزة (DER)-المرمزة PKCS#7 المحولة إلى Base64. إذا كان أسلوب POST مدعوما، فقد يتم إرسال المحتوى الذي سيتم إرساله في ترميز Base64 باستخدام GET بتنسيق ثنائي مع POST بدلا من ذلك.

عرض تخطيطي

القيم المحتملة **للعمليات** وقيم **الرسائل المقترنة بها**:

- **العملية** = `PKIOpresence`: **رسالة**وهي كل SCEP **pkiMessage**، بناء على PKCS#7 ومرمز Base64.يمكن أن تكون بنية **PkiMessage** من هذه الأنواع: **PKCSReq**: باستخدام DER و PKCS#10 CSR**GetCertInitial**: إستطلاع حالة من CSR**GetCert** أو **GetCRL**: الشهادة أو إسترداد CRL
- **العملية** = **GetCACert**، **GetNextCACert**، أو (إختياري) **GetCACap**: يمكن حذف **الرسالة**، أو يمكن تعيينها على اسم يعرف المرجع المصدق.

استجابات SCEP

تنسيق رسالة الاستجابة

يتم إرجاع استجابات SCEP كمحتوى HTTP قياسي، مع **نوع المحتوى** الذي يعتمد على الطلب الأصلي ونوع البيانات التي تم إرجاعها. يتم إرجاع محتوى DER كثنائي (ليس في Base64 كما هو الحال بالنسبة للطلب). قد يحتوي محتوى PKCS#7 أو قد لا يحتوي على بيانات (شهادات)، في مشفرة/موقعة مغلفة، إذا لم يحتوي على (يحتوي فقط على مجموعة من الشهادات)، فيشار إليه باسم **PKCS#7 منحط**.

أنواع المحتوى

القيم المحتملة **لنوع المحتوى**:

التطبيق/x-pki-message:

- إستجابة لعملية **PKIOpresence**، مع **PKImessage** من النوع: **PKCSReq** أو **GetCertInitial** أو **GetCert** أو **GetCRL**
- نص الاستجابة هو **PKImessage** من النوع: **CertRep**

التطبيق/x-x509-ca-cert:

- رد على عملية GetCACert
- نص الاستجابة هو شهادة CA X.509 المرمزة من قبل DER

التطبيق/x-x509-ca-ra-cert:

- رد على عملية GetCACert
- نص الاستجابة هو PKCS#7 منحط مرمز من قبل DER يحتوي على شهادات CA و RA

التطبيق/x-x509-next-ca-cert:

- رد على عملية GetNextCACert
- نص الاستجابة هو تباين PKImessage من النوع: CertRep

بنية PkiMessage

SCEP OIDs

```
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
```

رسالة SCEP

- PKCS#7 SignedData
- PKCS#7 EnvelopeData (تسمى PKCSpkiPKInvelope؛ إختياري، مشفر إلى مستلم الرسالة)
  MessageData (CSR و CERT و CRL و ...)
- SignerInfo مع سمات مصدق عليها:
  TransactionID، MessageType، SenderNoncepkiStatus، recipientNonce (الاستجابة فقط)FailInfo (الاستجابة + الفشل فقط)

SCEP MessageType

- طلب:
  PKCSReq (19): PKCS#10 CSRGetCertInitial (20): إستطلاع تسجيل الشهادةGetCert (21): إستردادالشهادةGetCRL (22): إستردادCRL
- الجواب:
  CertRep (3): الاستجابة للشهادة وأ طلب CRL

SCEP PKIstatus

- الناجح (0): تم منح الطلب (الاستجابة في PKCSpkiNvelope)
- الفشل (2): رفض الطلب (التفاصيل في سمة FailInfo)
- معلق (3): الطلب ينتظر الموافقة اليدوية

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).