تكوين الشهادات الموقعة من CA باستخدام IOS XE PKI

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

تكوين IOS XE PKI

إنشاء مفتاح التشفير

نقطة الثقة crypto pki

تسجيل PKI للتشفير

مصدق تشفير pki

استيراد PKI للتشفير

مصادقة شهادات المرجع المصدق الظيري

مصادقة شهادة متوسطة واحدة أو أكثر

التحقق

استكشاف الأخطاء وإصلاحها

مفاهيم IOS PKI المتقدمة

استيراد شهادة بتنسيق PKCS12

تصدير شهادات PKCS12 أو PEM

تصدير مفاتيح RSA

استيراد مفاتيح RSA المولدة خارج المربع

حذف مفاتيح RSA

الأسئلة المتكررة

كيفية إنشاء CSR من شهادات متعددة في سلسلة واحدة أو CSR إلى شهادة موقعة ذاتيًا؟

كيفية إنشاء CSR على TrustPoint إلى شهادة الهوية الموجودة؟

المقدمة

يصف هذا المستند كيفية تكوين شهادات IOS XE الموقعة من قبل مرجع مصدق تابع لجهة خارجية (CA).

يوضح هذا المستند كيفية إستيراد سلسلة CA موقعة متعددة المستويات كما هو الحال بالنسبة للجهاز الذي يعمل كشهادة هوية (ID) بالإضافة إلى كيفية إستيراد شهادات الطرف الثالث الأخرى بغرض التحقق من صحة الشهادة.

المتطلبات الأساسية

المتطلبات

يجب تكوين NTP ووقت الساعة عند إستخدام ميزات IOS PKI.

إذا لم يقم المرسوم بتكوين NTP، قد تواجه مشاكل في إنشاء شهادة مع تاريخ/وقت مستقبلي/ماضي. يمكن أن يتسبب هذا الانحراف في التاريخ أو الوقت في حدوث مشاكل إستيراد ومشاكل أخرى على الطريق.

نموذج تكوين NTP:

```
ntp server 192.168.1.1
clock timezone EST -5
clock summer-time EDT recurring
```

المكونات المستخدمة

- موجه Cisco الذي يشغل برنامج Cisco IOS® XE17.11.1a

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

لاحظ أن بعض الميزات المفصلة في هذا المستند قد لا تتوفر في إصدارات IOS XE القديمة. حيث يكون قد تم الحرص على توثيق عند تقديم أمر أو ميزة أو تعديلها.

ارجع دائما إلى الوثائق الرسمية لميزات IOS XE PKI الخاصة بإصدار معين لفهم أي قيود أو تغييرات قد تكون ذات صلة بالإصدار الخاص بك:

الأمثلة:

- IOS 15 M/T: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-pki-overview.html
- IOS XE 16.12.x: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16-12/sec-pki-xe-16-12-book/sec-est-client-supp-pki.html
- IOS XE 17.x: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-pki-overview-0.html

تكوين IOS XE PKI

يجب على المرسوم على مستوى عال تنفيذ الإجراءات التالية عند العمل باستخدام شهادات PKI لبرنامج IOS XE:

1. إنشاء مفتاح للاستخدام مع ميزة أو خدمة (إنشاء مفتاح التشفير)
2. قم بتكوين نقطة ثقة باستخدام معلمات مختلفة وارتباط المفاتيح. (crypto pki trustPoint)
3. إنشاء طلب توقيع شهادة (CSR) (تسجيل PKI للتشفير)
4. تقديم CSR إلى مرجع مصدق للتوقيع (غير المغطى في هذا المستند)
5. مصادقة شهادات CA الجذر و/أو الوسيطة (مصادقة PKI للتشفير)
6. إستيراد شهادات الجهاز (إستيراد PKI للتشفير)
7. إختياري: مصادقة شهادات CA للنظير (مصادقة PKI للتشفير)

هذه الخطوات مفصلة في الأقسام القادمة مجمعة حسب الأوامر المطلوبة للإجراء المعطى.

إنشاء مفتاح التشفير

قام العديد من المسؤولين بإدخال هذا الأمر لتمكين Secure Socket Shell (SSH) على موجه أو كجزء من دليل تكوين لميزة ما. ومع ذلك فإن قلة منهم لم يشرحوا فعليا ما تقوم به هذه الأوامر.

خذ على سبيل المثال الأوامر التالية:

```
crypto key generate rsa general-keys modulus 2048 label rsaKey exportable
crypto key generate ec keysize 521 exportable label ecKey
```

سيؤدي تقسيم هذه الأوامر إلى أجزاء معينة إلى تفاصيل الاستخدام:

- يرشد الجزء الأول من الأمر بالأسود (إنشاء مفتاح التشفير) الموجه إلى أننا سنقوم بإنشاء مفتاح جديد. هناك خيارات أخرى مثل تصدير مفتاح التشفير أو إستيراد مفتاح التشفير أو حجم مفتاح التشفير التي سيتم تفصيلها لاحقا.
- يرشد الجزء التالي من الأمر في green (rsa general-keys، ec) الموجه نوع المفتاح الذي نقوم بإنشائه بالضبط. سيتم إستخدام زوج مفاتيح Rivest-Shamir-Adleman (RSA) الذي يتكون من مفتاح عام/خاص ولكن يمكن أيضا للمؤول تكوين المنحنى الاهليلجي (EC) للاستخدام مع ميزات مثل تلك التي تتطلب شهادات ECDSA أو للاستخدام مع مصافحة ECDHE.
- يحدد الأمر البرتقالي حجم مفاتحنا.
  - بالنسبة إلى RSA، فإن المعامل هو المصطلحات والقيم التي تتراوح بين 512 و 4096 هي الخيارات المتاحة. يختلف حجم المعامل الافتراضي حسب الإصدار ولكن يقترح اتباع أفضل ممارسة ل Cisco لتشفير الجيل التالي واستخدام مفاتيح أكبر من 2048.
  - بالنسبة إلى EC، يلزم الأمر key-size لتحديد عدد وحدات بت في المفاتح. الخيارات هي 256، 384، أو 512.
- يحدد الأمر بالبنفسجي التسمية الخاصة بهذا المفاتح. وهذا أمر مهم لأن المؤول قد يحتاج إلى تحديد مفاتيح متعددة لأغراض مختلفة على جهاز IOS XE نفسه. يتم إستخدام التسمية لتحديد المفاتح الدقيق للاستخدام مع ميزة معينة. حيثما كان ذلك ممكنا، أستخدم دائما علامة لتمييز المفاتيح المستخدمة وجعل تعيين المفاتيح للميزات أسهل بكثير. على سبيل المثال: سيقوم كل من SSH للتسمية و CUBE للتسمية و HTTPS بإنشاء مفاتيحين للاستخدام مع خدمات أو ميزات مختلفة.

- التسمية الافتراضية لمفتاح هي اسم الأجهزة hostname.domain. قد تقوم بعض الأجهزة بإنشاء مفاتيح RSA على التمهيد الأول. من خلال عدم إدخال إصلاح للتسمية، قد يكون المسؤول معرضا لخطر الكتابة/إعادة إنشاء المفاتيح الحالية بشكل غير مقصود
- الأمر الأخير باللون الأزرق هو الباعة القابل للتصدير. يوضح هذا الأمر بالتفصيل أنه يمكن إستخدام المفاتيح مع الأمر crypto pki export للتصدير والاستخدام مع الأنظمة الأخرى. وقد يكون أحد الأمثلة على ذلك هو الاستيراد إلى جهاز نظير فائق التوفر، لذلك يتم إستخدام مفتاح واحد بواسطة كل من أعضاء زوج HA أو للاستخدام داخل أدوات المستندة إلى TLS مثل Wireshark لفك تشفير جلسات إستكشاف الأخطاء وإصلاحها. أيا كان السبب الذي يجب قوله إنه يمكن إنشاء مفاتيح RSA كقابلة للتصدير RSA. الفقط من البداية. إذا قام المسؤول بإنشاء مفتاح RSA غير قابل للتصدير، مما يمكن تعيين هذا المفتاح على أنه قابل للتصدير دون إعادة إنشاء المفتاح، قد يؤدي إلى تأثير التوازي على ميزات أخرى مثل إبطال جميع الشهادات التي تم إنشاؤها باستخدام هذا المفتاح. ومع ذلك، يمكن خفض مستوى المفتاح القابل للتصدير إلى غير قابل للتصدير دون إعادة إنشاء المفتاح باستخدام الأمر crypto key move rsaKeyLabel غير قابل للتصدير

أمثلة التكوين:

<#root>

```
Router(config)#

crypto key generate rsa general-keys modulus 2048 label rsaKey exportable

The name for the keys will be: rsaKey

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)

Router(config)#

crypto key generate ec keysize 521 exportable label ecKey

The name for the keys will be: ecKey
```

أمثلة التحقق:

<#root>

```
Router#

show crypto key mypubkey rsa rsaKey

% Key pair was generated at: 10:21:42 EDT Apr 14 2023
Key name: rsaKey
Key type: RSA KEYS      2048 bits
 Storage Device: not specified
 Usage: General Purpose Key
 Key is exportable. Redundancy enabled.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
```

```
  [..truncated..]
  9F020301 0001

Router#

show crypto key mypubkey ec ecKey

% Key pair was generated at: 10:03:05 EDT Apr 14 2023
Key name: ecKey
Key type: EC KEYS      p521 curve
 Storage Device: private-config
 Usage: Signature Key
 Key is exportable. Redundancy enabled.
 Key Data:
  30819B30 1006072A 8648CE3D 02010605 2B810400 23038186 000401A2 A77FCD34
  [..truncated..]
  93FAC967 96ADA79E 4A245881 B2AD2F4A 279A362D F390A20F C06D5845 06DA
```

نقطة الثقة crypto pki

نقاط الثقة هي مفهوم "يشبه المجلد" لتخزين وإدارة شهادات PKI ضمن IOS XE. (صيغة الأمر)

على مستوى عال:

1. يمكن أن يحتوي كل IOS XE TrustPoint على شهادة CA أحادية الجذر أو متوسطة الحجم يتم تحميلها بواسطة أمر مصادقة pki crypto. اعتبر أن نقاط الثقة المصدق عليها هي إضافة شهادات موثوق بها الآن من قبل الجهاز.
2. يمكن لكل IOS XE TrustPoint أيضا إستيراد شهادة هوية واحدة (ID) محملة بطريقة أمر إستيراد PKI للتشفير. شهادة الهوية هي شهادة هذه الأجهزة التي ترتبط عادة بخدمة أو ميزة ما.
3. يمكن أن يستخدم المسؤول الأمر authenticate وimport على نفس TrustPoint (والمطلوب لاستيراد شهادة معرف تمت مناقشتها لاحقا.) عند إستخدام سير عمل المصادقة/الاستيراد، ستحتوي TrustPoint على شهادتين (الجذر/الوسيط + شهادة الهوية).
4. عند إستخدام نقاط الثقة لغرض تخزين شهادات CA الوسيطة/الجذر الظير الموثوق بها فقط مصدق تشفير pki الأمر مطلوب. في هذا السيناريو، سوف تحتوي نقطة الثقة فقط على الشهادة الفردية التي تم التصديق عليها من قبل المسؤول.

ملاحظة: سوف توفر الأقسام التالية لمصادقة PKI وإستيراد PKI المشفرة والأقسام اللاحقة التي توضح أمثلة المصادقة/الاستيراد للشهادات متعددة المستويات المزيد من السياق لهذه النقاط الأربعة.

يمكن أن يكون لنقاط الاتصال أوامر مختلفة تم تكوينها. يمكن إستخدام هذه الأوامر للتأثير على القيم الموجودة داخل طلب توقيع الشهادة (CSR) الذي تم إنشاؤه بواسطة الجهاز باستخدام الأمر crypto pki enroll على نقطة موثوق بها.

هناك العديد من الأوامر المختلفة المتوفرة لنقطة الثقة (كثيرة جدا بحيث ال يمكن تفصيلها في هذا المستند) ولكن هناك بعض الأمثلة الأكثر شيوعا موضحة في كل من المثال TrustPoint والجدول أدناه:

```
crypto pki trustpoint labTrustpoint
 enrollment terminal pem
 serial-number none
 fqdn none
 ip-address none
 subject-name cn=router.example.cisco.com
 subject-alt-name myrouter.example.cisco.com
 revocation-check none
 rsakeypair rsaKey
 hash sha256
```

	الوصف
crypto pki trustPoint labTrustPoint	تسمية التكوين القابل للقراءة للبشرية نقطة الاتصال هذه. يستخدم للارتباط بميزات وأ خدمات في أوامر لاحقة.
PEM الطرفي للتسجيل	تحديد الإجراء الذي سيقوم به أمر تسجيل PKI للتشفير. في هذا المثال يشير PEM الطرفي للتسجيل إلى أن طلب توقيع الشهادة (CSR) سيتم إخراجه إلى المحطة الطرفية في نص بتنسيق PEM ل Base64. يمكن إستخدام خيارات أخرى مثل شهادة التسجيل المقوع ذاتيا إلنشاء عنوان تكويني يمكن توقيعه ذاتيا وأ عنوان URL لتحديد عنوان URL للتسجيل لوكوتورب من ةفادتسالاو HTTP للتسجيل الشهادة البسيط (SCEP). اذه قاطن جارخ الطريقتين الكل المستند.
الرقم التسلسلي الب	تحديد ما إذا كان سيتم إضافة CSR أم ال. أجهزة IOS XE إلى تسلسل رأمألا موجه ليطعت إلى اضيأ اذه يؤدي إلى تشفير PKI لتسجيل رمأ ءانثأ.
fqdn none	تحديد ما إذا كان سيتم إضافة اسم المجال المؤهل بالكامل (FQDN) إلى CSR أم ال. يؤدي اذه إلى تعطيل اضيأ إلى PKI لتسجيل رمأ ءانثأ رمأ الأمر موجه لتشفير.
عنوان IP الب	تحديد ما إذا كان سيتم إضافة عنوان IP إلى CSR أم ال. يؤدي اذه إلى تعطيل اضيأ إلى أجهزة IOS XE لتسجيل رمأ ءانثأ رمأ الأمر موجه لتشفير.

	هذا أيضا إلى تعطيل موجه الأمر أثناء تسجيل PKI للتشفير.
اسم الموضوع cn=router.example.cisco.com	يشير إلى تنسيق X500 الذي ستتم إضافته إلى CSR.
subject-alt-name myrouter.example.cisco.com	بدءا من IOS XE 17.9.1 يمكن إضافة قيم اسم بديل للموضوع (SAN) إلى CSR.
revocation-check none	يشير إلى كيفية التحقق من صحة الشهادة من قبل جهاز IOS XE. يمكن استخدام خيارات مثل إبطال قائمة الشهادات (CRL) وبروتوكول حالة الشهادة عبر الإنترنت (OCSP) إذا كانت مدعومة من قبل المرجع المصدق الذي يختاره. ويتم استخدام هذا الأمر بشكل أساسي عند استخدام TrustPoint من قبل تم تكوينها مسبقا أو خدمة أخرى IOS XE. كما يتم التحقق من حالة الإبطال عند مصادقة الشهادة باستخدام TrustPoint.
rsakeypair rsaKey	يشير الأمر المستخدم لتحديد مفاتيح RSA التي سيتم استخدامها مع هذه التسمية المحددة. تستخدم أوامر شهادات ECDSA "eckeypair ecKey" التي تشير إلى تسمية مفاتيح EC
تجزئة SHA256	يؤثر هذا الأمر على نوع خوارزمية التجزئة المراد استخدامها. الخيارات هي SHA512 و SHA384 و SHA256 و SHA1

تسجيل PKI للتشفير

يتم إستخدام الأمر crypto pki login لتشغيل أمر التسجيل على نقطة موثوق بها معينة. (رمز الاستجابة السريعة)
على سبيل المثال، سيقوم الأمر crypto pki enroll labTrustPoint بعرض طلب توقيع الشهادة (CSR) على الوحدة الطرفية بتنسيق نص Base64 PEM كما هو موضح في المثال التالي.

يمكن الآن حفظ طلب توقيع الشهادة هذا في ملف نصي وأو نسخة ولصقه من سطر الأوامر للتحقق من الصحة والتوقيع لأي جهة خارجية.

```
<#root>

Router(config)#

crypto pki enroll labTrustpoint

% Start certificate enrollment ..
```

```
% The subject name in the certificate will include: cn=router.example.cisco.com
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwIzEhMB8GA1UEAxMYcm91dGVyLmV4YW1wbGUuY2lzY28uY29t
[..truncated..]
mGvBGUpn+cDIdFcNVzn8LQk=
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---
```

مصدق تشفير pki

يتم إستخدام الأمر crypto pki authenticate لإضافة شهادة CA موثوق بها إلى نقطة موثوق بها عينة. يمكن مصادقة لك نقطة ثقة مرة واحدة. أي، يمكن أن تحتوي TrustPoint فقط على جذر CA واحد أو شهادة وسيطة. سيؤدي تشغيل الأمر مرة ثانية وإضافة شهادة جديدة إلى الكتابة فوق الشهادة الأولى.

باستخدام الأمر register terminal pem الذي تم تكوين الأمر crypto pki authenticate سيطالب المستخدم بشهادة بتنسيق PEM للأساس 64 يتم تحميلها عبر CLI. (أمر الإغاء)

يمكن أن يقوم المسؤول بمصادقة TrustPoint لإضافة الشهادات الوسيطة الاختيارية والجذرية في سلسلة شهادات بغرض إستيراد شهادة معرف الجهاز الحالي.

قد يقوم المسؤولون أيضا بمصادقة TrustPoint لإضافة مراجع مصدقة أصلية موثوقة أخرى إلى جهاز IOS XE بغرض تمكين العلاقات الثقة مع أجهزة النظير أثناء عمليات تبادل للبروتوكول مع جهاز النظير هذا.

ولمزيد من التوضيح، يمكن أن يكون لجهاز النظير سلسلة شهادات موقعة من قبل "Root CA 1". للتحقق من صحة الشهادة أثناء مصافحة البروتوكول بين جهاز IOS XE وجهاز النظير للنجاح؛ يمكن للمسؤول إستخدام الأمر crypto pki authenticate لإضافة شهادة CA إلى نقطة موثوق بها على جهاز IOS XE.

العنصر الرئيسي الذي يجب تذكره: مصادقة نقاط الثقة باستخدام مصادقة PKI للتشفير وه دائما إضافة شهادات جذر CA أو الشهادات الوسيطة إلى نقطة اتصال، وليس إضافة شهادات الهوية. الحظ أن هذا المفهوم يطبق أيضا على مصادقة الشهادات الموقعة ذاتيا من جهاز نظير آخر.

يوضح المثال التالي كيفية مصادقة نقطة ثقة من إصدارات سابقة باستخدام الأمر crypto pki authenticate:

<#root>

```
Router(config)#
```

crypto pki authenticate labTrustpoint

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: C955FC74 7AABC184 D8A75DE7 3C9E7218
      Fingerprint SHA1: 3A99FF61 1E9E6C7B D0E567A9 96D882F5 2279C534

% Do you accept this certificate? [yes/no]:

yes

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

إستيراد PKI للتشفير

يتم إستخدام هذا الأمر لاستيراد شهادة الهوية (ID) إلى TrustPoint. يمكن لنقطة ثقة واحدة أن تحتوي على شهادة معرف واحد فقط وسيؤدي إصدار الأمر مرة ثانية إلى المطالبة باستبدال الشهادة التي تم إستيرادها مسبقا. (رمز الأمر)

يوضح المثال التالي كيفية إستيراد شهادة هوية إلى مثال TrustPoint من قبل باستخدام أمر إستيراد PKI crypto.

<#root>

```
Router(config)#

crypto pki import labTrustpoint certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

سيحصل المسؤول على خطأ عند محاولة إستيراد شهادة قبل أن يقوم TrustPoint بمصادقة شهادة المرجع المصدق المستخدمة لتوقيع هذه الشهادة مباشرة.

<#root>

```
Router(config)#

crypto pki import labTrustpoint certificate

% You must authenticate the Certificate Authority before
 you can import the router's certificate.
```

مصادقة شهادات المرجع المصدق النظير

تتم إضافة شهادات المرجع المصدق النظير إلى IOS XE باستخدام نفس الطريقة لإضافة أي شهادة CA. وهذا يعني، أنه يتم مصادقتها مقابل نقطة اتصال باستخدام الأمر crypto pki authenticate.

يوضح الأمر أدناه كيفية إنشاء نقطة ثقة ومصادقة شهادة مرجع مصدق من طرف ثالث نظير.

1. قم بإنشاء نقطة ثقة مع بعض الاسم الوصفي الذي سيحمل شهادة المرجع المصدق النظير
2. قم بتكوين PEM terminal للتسجيل حتى يطلب الأمر crypto pki authenticate الشهادة عبر سطر الأوامر.
3. تكوين إلغاء-التحقق من none لتخطي التحقق من CRL/OCSP أثناء عملية الاستيراد
4. مصادقة TrustPoint وتوفير الشهادة
5. كرر الخطوات من 1 إلى 4 حسب ما هو مطلوب لشهادات المرجع المصدق النظير (تذكر!) نقطة اتصال لكل فقط واحدة مصدق مرجع شهادة

```
<#root>

Router(config)#

crypto pki trustpoint PEER-ROOT

Router(ca-trustpoint)#

enrollment terminal pem

Router(ca-trustpoint)#

revocation-check none



Router(ca-trustpoint)#

crypto pki authenticate PEER-ROOT


Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: 62D1381E 3E03D06A 912BAC4D 247EEF17
      Fingerprint SHA1: 3C97CBB4 491FC8D6 3D12B489 0C285481 64198EDB

% Do you accept this certificate? [yes/no]:

yes


Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

مصادقة شهادة متوسطة واحدة أو أكثر

توضح الأمثلة السابقة كيفية إنشاء CSR باستخدام تسجيل PKI للتشفير، ومصادقة شهادة CA الجذر باستخدام مصادقة PKI للتشفير، ثم إستيراد شهادة الهوية باستخدام إستيراد PKI للتشفير.
غير أنه عند إدخال شهادات وسيطة، تختلف العملية إختلافا طفيفا. الـ تخف، الـ تزال المفاهيم والاوامر نفسها مطبقة! يكمن الاختلاف في كيفية تحديد نقاط الثقة التي تحتفظ بالشهادات.

تذكر أن كل TrustPoint يمكن أن يحتوي فقط على شهادة CA جذر أو متوسط. لذلك في مثال حيث لديك سلسلة CA مثل أسفل التي تظهر أدناه، من المستحيل إستخدام أمر مصادقة تشفير PKI لإضافة أكثر من شهادة CA:

<#root>

```
- Root CA
```

```
 - Intermediate CA 1
```

```
   - Identity Certificate
```

الحل:

1. قم بإنشاء نقطة ثقة تحتفظ ب CA الجذر الذي تمت مصادقته.
2. ثم مصادقة الشهادة الوسيطة باستخدام TrustPoint المستخدمة لإنشاء CSR
3. وأخيرا قم باستيراد شهادة الهوية إلى نقطة الثقة النهائية.

باستخدام الجدول الموجود أدناه، يمكن توضيح الشهادة التي تطلب تعيين TrustPoint بألوان تتوافق مع السلسلة السابقة للمساعدة في التصور.

اسم الشهادة	TrustPoint المطلوب إستخدامه	أمر الاستخدام
المرجع المصدق الجذر	crypto pki trustPoint root-ca	مصادقة ROOT-CA لتشفير PKI
CA 1 الوسيط	crypto pki trustPoint labTrustPoint	crypto pki authenticate labTrustPoint
شهادة الهوية	crypto pki trustPoint labTrustPoint	شهادة إستيراد LabTrustPoint ل crypto PKI

يمكن تطبيق نفس المنطق على سلسلة شهادات ذات شهادتي CA متوسطتين. مرة أخرى يتم توفير الألوان للمساعدة في عرض مكان تطبيق المرجع المصدق الوسيط الجديد على

تكوين IOS XE.

<#root>

- Root CA

- Intermediate CA 1

- Intermediate CA 2

- Identity Certificate

اسم الشهادة	TrustPoint المطلوب إستخدامه	أمر الاستخدام
المرجع المصدق الجذر	crypto pki trustPoint root-ca	مصادقة ROOT-CA لتشفير PKI
CA 1 الوسيط	crypto pki trustPoint inter-ca	CRYPTO PKI Authenticate INTER CA
CA 2 الوسيط	crypto pki trustPoint labTrustPoint	crypto pki authenticate labTrustPoint
شهادة الهوية	crypto pki trustPoint labTrustPoint	شهادة إستيراد LabTrustPoint ل crypto PKI

عند النظر عن كثب يمكن للمرء أن يلاحظ نمطين:

1. يتم تحميل جميع الشهادات الجذر أو الوسيطة في نقاط الثقة باستخدام مصادقة PKI للتشفير (بغض النظر عن عدد تلك الشهادات).
2. كما يمكن ملاحظة أن الشهادة النهائية قبل شهادة هوية الجهاز (قراءة الشهادة التي وقعت مباشرة على شهادة الهوية) مصدق عليها دائما على نفس نقطة الثقة حيث يتم إستيراد شهادة الهوية.
   - على غرار الخطأ الذي تم عرضه سابقا، لن يسمح IOS XE للمسؤول باستيراد شهادة بدون مصادقة شهادة CA المستخدمة لتوقيع هذه الشهادة مباشرة.

يمكن إستخدام هذين النمطين أعلاه لأي عدد من الشهادات الوسيطة يتجاوز النمطين، رغم أنه من المحتمل أن يرى المسؤول في معظم عمليات النشر أكثر من نمطين من الشهادات المصدقة الوسيطة في سلسلة الشهادات.

للحصول على الاكتمال، يتم توفير جدول شهادة الجذر/الهوية التالي أيضا:

<#root>

- Root CA

```
- Identity Certificate
```

اسم الشهادة	TrustPoint المطلوب إستخدامه	أمر الاستخدام
المرجع المصدق الجذر	crypto pki trustPoint labTrustPoint	crypto pki authenticate labTrustPoint
شهادة الهوية	crypto pki trustPoint labTrustPoint	شهادة إستيراد LabTrustPoint ل crypto PKI

التحقق

- أثناء عملية المصادقة أو الاستيراد، يتم إجراء العديد من عمليات التحقق من سلامة النظام من قبل IOS XE لضمان صحة الشهادة وتكوينها بشكل جيد. ستتم طباعة هذه الأخطاء على الشاشة أو السجلات (show logging) للبحث عن البنود التي تبدأ ب "crypto_PKI"

وفيما يلي بعض الأمثلة الشائعة:

يتم إجراء عمليات الفحص الصحيحة قبل/بعد استناد إلى الوقت الذي تم تكوينه مقارنة بالوقت الموجود في الشهادة

```
<#root>

004458:

Aug  9

 21:05:34.403: CRYPTO_PKI: trustpoint labTrustpoint authentication status = 0

%CRYPTO_PKI: Cert not yet valid or is expired -

    start date: 05:54:04 EDT

Aug 29

 2019
    end   date: 05:54:04 EDT Aug 28 2022
```

إذا لم يتم تعطيل التحقق من الإبطال، سيقوم IOS XE بفحص الإبطال من خلال الطريقة التي تم تكوينها قبل إستيراد الشهادة

```
<#root>

003375: Aug  9 20:24:14:

%PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint ROOT failed

003376: Aug  9 20:24:14.121:

CRYPTO_PKI: enrollment url not configured
```

لعرض تفاصيل حول تكوين TrustPoint، وأ التي تمت مصادقتها، وأ إستيرادها، أستخدم الأوامر أدناه:

```
show crypto pki trustpoints trustpoint_name
show crypto pki certificates trustpoint_name
show crypto pki certificates verbose trustpoint_name
```

استكشاف الأخطاء وإصلاحها

عند تصحيح مشاكل الاستيراد أو مشاكل PKI الأخرى، يستخدم تصحيح الأخطاء التالية.

```
debug crypto pki messages
debug crypto pki transactions
debug crypto pki validation
debug crypto pki api
debug crypto pki callback
!
debug ssl openssl error
debug ssl openssl msg
debug ssl openssl states
debug ssl openssl ext
```

مفاهيم IOS PKI المتقدمة

إستيراد شهادة بتنسيق PKCS12

قد توفر بعض موفري CA المفلفات مرة أخرى بتنسيق PKCS#12 (.pfx، .p12).

PKCS#12 هو نوع خاص من أشكال الشهادات حيث يتم تجميع سلسلة الشهادات بأكملها من الشهادة الجذر إلى شهادة الهوية مع زوج مفاتيح RSA.

هذه التنسيق مفيد جدا للاستيراد باستخدام IOS XE ويمكن إستيراده بسهولة باستخدام الأمر أدناه:

<#root>

```
Router(config)#
```

crypto pki import PKCS12-TP pkcs12 terminal password Cisco123

or

```
Router(config)#
```

crypto pki import PKCS12-TP pkcs12 ftp://cisco:cisco@192.168.1.1/certificate.pfx password Cisco123

```
% Importing pkcs12...
Address or name of remote host [192.168.1.1]?
Source filename [certificate.pfx]?
Reading file from ftp://cisco@192.168.1.1/certificate.pfx!
[OK - 2389/4096 bytes]
% You already have RSA keys named PKCS12.
% If you replace them, all router certs issued using these keys
% will be removed.
% Do you really want to replace them? [yes/no]:
```

yes

```
CRYPTO_PKI: Imported PKCS12 file successfully.
```

تصدير شهادات PKCS12 وأ PEM

يمكن أن يصدر المسؤول الشهادات إلى المحطة الطرفية على هيئة تنسيق PEM لنص عادي Base64 أو نص عادي مشفر Base64 أو PKCS12 للاستيراد إلى أجهزة نظيرة أخرى.

ويكون هذه الإجراء مفيدا عند عرض أجهزة نظير جديدة ويحتاج المسؤول إلى مشاركة شهادة مرجع مصدق جذري وقعت على شهادة هوية الأجهزة.

فيما يلي بعض نماذج الصياغة:

<#root>

```
Router(config)#
```

crypto pki export labTrustpoint pem terminal

```
Router(config)#
```

crypto pki export labTrustpoint pem terminal 3des password Cisco!123

```
Router(config)#
```

crypto pki export labTrustpoint pkcs12 terminal password cisco!123

تصدير مفاتيح RSA

قد يكون مطلوبا لتصدير مفاتيح RSA للاستيراد إلى جهاز آخر أو للاستخدام في جهود أستكشاف الأخطاء وإصلاحها. يمكن تصدير المفاتيح باستخدام أمر تصدير مفاتيح التشفير مع طريقة تشفير (DES، 3DES، AES) وكلمة مرور.

إستخدام النموذج:

<#root>

```
Router(config)#
```

```
crypto key export rsa rsaKey pem terminal aes Cisco!123

% Key name: IOS-VG
   Usage: General Purpose Key
   Key data:
-----BEGIN PUBLIC KEY-----
[..truncated..]
-----END PUBLIC KEY-----

base64 len 1664-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,40E087AFF0886DA7C468D2084A0DECFB

[..truncated..]
-----END RSA PRIVATE KEY-----
```

إذا لم يكن المفتاح قابلا للتصدير، سيظهر خطأ.

```
<#root>

Router(config)#

crypto key export rsa kydavis.cisco.com pem terminal 3des mySecretPassword


% RSA keypair kydavis.cisco.com' is not exportable.
```

إستيراد مفاتيح RSA المولدة خارج المربع

قد يقوم بعض المسؤولين بتنفيذ RSA وإنشاء الشهادة خارج المربع، من الممكن إستيراد مفاتيح RSA باستخدام أمر إستيراد مفتاح التشفير كما هو موضح أدناه باستخدام كلمة المرور.

```
<#root>

Router(config)#

crypto key import rsa rsaKey general-purpose exportable terminal mySecretPassword

% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
[..truncated..]
-----END PUBLIC KEY-----

% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9E31AAD9B7463502
[..truncated..]
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.
```

حذف مفاتيح RSA

أستخدم الأمر crypto key zeroize rsa rsaKey لحذف زوج مفاتيح RSA باسم rsaKey.

إستيراد حزمة CA الموثوقة من Cisco من خلال TrustPool

تختلف بروتوكولات الثقة بشكل طفيف عن أي نقطة ثقة ولكن الاستخدام الأساسي هو نفسه. عندما تحتوي نقاط الثقة عادة على شهادة CA واحدة، سوف يحتوي تجمع الثقة على عدد من CAs الموثوق بها.

تنشر Cisco حزم CA على https://www.cisco.com/security/pki/

أحد الاستخدامات الشائعة هي تنزيل ملف ios_core.p7b باستخدام الأمر أدناه:

<#root>

```
Router(config)#

crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_core.p7b

Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
% PEM files import succeeded.
Router(config)#
```

الأسئلة المتكررة

هل يؤدي حذف نقطة ثقة إلى إبطال CSR أو سلسلة شهادات تم منحها من CSR معينة؟

لا، بمجرد إنشاء CSR وحفظها، يمكن حذف TrustPoint وإعادة إضافتها دون إبطال CSR.

غالبا ما يتم إستخدام هذا الأمر من قبل الدعم الفني من Cisco لبدء تشغيل جديد عند حدوث خطأ في مصادقة/إستيراد الشهادات.

طالما لا يقوم المسؤول أو مهندس الدعم بإعادة إنشاء مفاتيح RSA، يمكن إستيراد CSR أو سلسلة الشهادات الموقعة لمصادقة/إستيراد.

هام! ستؤدي إزالة TrustPoint إلى حذف أي شهادات مصدق عليها/مستوردة والتي قد تكون أكثر إشكالية بافتراض أن هذه الشهادات قيد الاستخدام حاليا من قبل خدمة أو ميزة ما.

هل سيؤدي إنشاء CSR على TrustPoint إلى إبطال الشهادة الموجودة؟

لا، هذا شائع عندما تكون الشهادات على وشك الانتهاء. يمكن أن يقوم المسؤول بتنفيذ أمر تسجيل PKI لإنشاء CSR جديد وبدء عملية توقيع الشهادة باستخدام CA بينما تظل الشهادات الموجودة التي تم مصادقتها/إستيرادها قيد الاستخدام. لحظة قيام المسؤول باستبدال الشهادات بمصادقة تشفير PKI/إستيراد PKI هي اللحظة التي يتم فيها

إستبدال الشهادات القديمة.

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).