IOS XE PKI를 사용하여 CA 서명 인증서 구성

목차

소개

이 문서는 서드파티 CA(Certificate Authority)에서 서명한 IOS XE 인증서를 구성하기 위한 일반 가이드 역할을 합니다.

이 문서에서는 디바이스가 ID(Identity) 인증서로 작동하도록 멀티 레벨 CA 서명 체인을 가져오는 방법과 인증서 검증을 위해 다른 서드파티 인증서를 가져오는 방법에 대해 자세히 설명합니다.

사전 요구 사항

요구 사항

IOS PKI 기능을 활용할 때 NTP 및 Clock time을 구성해야 합니다.

관리자가 NTP를 구성하지 않으면 미래/과거 날짜/시간으로 생성되는 인증서에 문제가 있을 수 있습니다. 날짜 또는 시간의 이러한 왜곡은 향후 가져오기 문제 및 기타 문제를 야기할 수 있습니다.

샘플 NTP 구성:

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

사용되는 구성 요소

- Cisco IOS® XE17.11.1a를 실행하는 Cisco 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에 설명된 일부 기능은 이전 IOS XE 버전에서 제공되지 않을 수 있습니다. 명령이나 기능이 도입되거나 수정되었을 때 문서화하는 데 주의해야 하는 경우

특정 버전과 관련될 수 있는 제한 또는 변경 사항을 파악하려면 항상 해당 버전의 IOS XE PKI 기능에 대한 공식 설명서를 참조하십시오.

예:

- 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

IOS XE PKI 컨피그레이션

상위 레벨에서 관리자는 IOS XE PKI 인증서를 사용할 때 다음 작업을 수행해야 합니다.

1. 기능 또는 서비스에 사용할 키 만들기(암호화 키 생성)
2. 다양한 매개변수로 신뢰 지점을 구성하고 키를 연결합니다. (crypto pki trustpoint)
3. CSR(Certificate Signing Request) 생성(crypto pki enroll)
4. 서명을 위해 CA에 CSR 제공(이 문서에서는 다루지 않음)
5. 루트 및/또는 중간 CA 인증서 인증(crypto pki 인증)
6. 디바이스 인증서 가져오기(crypto pki 가져오기)

7. 선택 사항: 피어 CA 인증서 인증(crypto pki authenticate)

이러한 단계는 다음 섹션에서 특정 작업에 필요한 명령을 그룹화하여 자세히 설명합니다.

암호화 키 생성

라우터에서 또는 기능에 대한 일부 컨피그레이션 가이드의 일부로 SSH(Secure Socket Shell)를 활성화하기 위해 많은 관리자가 이 명령을 입력했습니다. 그러나 그 명령이 실제로 무엇을 하는지 해부하지 않은 사람은 거의 없다.

아래 명령의 예를 들어 보겠습니다.

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

이러한 명령을 특정 부품으로 분류하면 사용법에 대해 자세히 설명합니다.

- 검정색(crypto key generate) 명령의 첫 번째 부분은 라우터에 새 키를 만들도록 지시합니다. 암호화 키 내보내기, 암호화 키 가져오기 또는 암호화 키 0과 같은 다른 옵션은 나중에 자세히 설명합니다.
- 녹색(rsa general-keys, ec) 명령의 다음 부분에서는 어떤 유형의 키를 생성하는지 라우터에 정확하게 지시합니다. 대부분의 경우 공용/개인 키로 구성된 RSA(Rivest-Shamir-Adleman) 키 쌍이 사용되지만 관리자는 ECDSA 인증서가 필요한 기능과 함께 사용하거나 ECDHE 핸드셰이크에 사용할 EC(Elliptic Curve)를 구성할 수도 있습니다.
- 주황색 명령은 키의 크기를 정의합니다.
  - RSA의 경우 모듈러스는 용어 및 512-4096 사이의 값을 사용할 수 있습니다. 기본 모듈러스 크기는 버전에 따라 다르지만 차세대 암호화를 위한 Cisco의 모범 사례를 따르고 2048년 이상의 키를 활용하는 것이 좋습니다.
  - EC의 경우 키의 비트 수를 지정하려면 key-size 명령이 필요합니다. 옵션은 256, 384 또는 512입니다.
- 보라색 명령은 이 키의 레이블을 정의합니다. 이는 관리자가 동일한 IOS XE 디바이스에서 다양한 용도로 여러 키를 정의해야 할 수 있기 때문에 중요합니다. 레이블은 지정된 기능에 사용할 정확한 키를 지정하는 데 사용됩니다. 가능한 경우 항상 레이블을 사용하여 사용 중인 키를 구별하고 기능에 키를 훨씬 쉽게 할당할 수 있습니다. 예를 들어 SSH 레이블 지정, CUBE 레이블 지정, HTTPS 레이블 지정은 서로 다른 서비스 또는 기능에 사용할 두 개의 키를 생성합니다.
  - 키의 기본 레이블은 devices hostname.domain입니다. 일부 디바이스는 첫 번째 부팅 시 RSA 키를 생성할 수 있습니다. 수정 후 레이블 입력을 하지 않으면 관리자가 실수로 잘못된 키를 덮어쓰거나 다시 생성할 위험이 있습니다
- 파란색으로 표시된 마지막 명령은 내보낼 수 있는 후위입니다. 이 명령에서는 키를 crypto pki export 명령과 함께 사용하여 내보내고 다른 시스템과 함께 사용할 수 있음을 자세히 설명합니다. 예를 들어, HA 쌍의 두 멤버 모두에서 단일 키를 사용하거나 Wireshark와 같은 트러블슈팅 툴 내에서 RSA 기반 TLS 세션을 해독하는 데 사용하기 위해 피어 고가용성 디바이스로 가져올 수 있습니다. 어떤 이유에서든 RSA 키는 처음부터 내보낼 수 있는 상태로만 만들 수 있습니다. 관리자가 내보낼 수 없는 RSA 키를 생성하는 경우 이 키를 다시 생성하지 않으면 내

보낼 수 있도록 설정할 수 없습니다. 그러면 해당 키를 사용하여 생성된 모든 인증서를 무효화하는 등 다른 기능에 영향을 미칠 수 있습니다. 즉, crypto key move rsaKeyLabel non-exportable 명령을 사용하면 키를 다시 생성하지 않고 내보낼 수 없는 키로 다운그레이드할 수 있습니다

컨피그레이션 예:

<#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
```

확인 예:

<#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
```

암호화 pki 신뢰 지점

신뢰 지점은 IOS XE 내에서 PKI 인증서를 저장하고 관리하기 위한 "폴더와 유사한" 개념입니다(명령 구문).

상위 레벨:

1. 각 IOS XE 신뢰 지점에는 crypto pki authenticate 명령을 통해 로드된 단일 루트 또는 중간 CA 인증서가 포함될 수 있습니다. 인증된 신뢰 지점을 디바이스에서 신뢰하는 인증서를 추가하는 것으로 간주합니다.
2. 각 IOS XE Trustpoint는 crypto pki import 명령을 통해 로드된 단일 ID(Identity) 인증서도 가져올 수 있습니다. ID 인증서는 일반적으로 일부 서비스 또는 기능에 연결되는 이 디바이스 인증서입니다.
3. 관리자는 동일한 신뢰 지점에서 authenticate and import 명령을 사용할 수 있습니다(이는 나중에 설명하는 ID 인증서를 가져오는 데 필요함). 인증/가져오기 워크플로를 사용할 때 신뢰 지점에는 두 개의 인증서(루트/중간 + ID 인증서)가 포함됩니다.
4. 신뢰 지점이 신뢰할 수 있는 피어 루트/중간 CA 인증서를 저장하기 위해 사용되는 경우 crypto pki 인증 명령이 필요합니다. 이 시나리오에서 신뢰 지점은 관리자가 인증한 단일 인증서만 포함합니다.

참고: 다음 섹션에서는 crypto pki authenticate and crypto pki import를 인증하고 다단계 인증서의 인증/가져오기 예를 자세히 설명합니다.

신뢰 지점에는 다양한 명령을 구성할 수 있습니다. 이러한 명령은 신뢰 지점에서 crypto pki enroll 명령을 사용하여 디바이스에서 생성한 CSR(Certificate Signing Request) 내의 값에 영향을 미칠 수 있습니다.

신뢰 지점에 사용할 수 있는 여러 가지 명령이 있습니다(이 문서에서는 자세히 설명하기에 너무 많음). 일반적인 몇 가지 예는 아래의 신뢰 지점 예와 표 모두에 자세히 설명되어 있습니다.

```
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
```

명령을 사용합니다	설명
crypto pki trustpoint labTrustpoint	이 신뢰 지점에 대한 사람이 읽을 수 있는 구성 레이블입니다. 이후 명령에서 기능

	또는 서비스에 연결하는 데 사용됩니다.
등록 터미널 pem	crypto pki enroll 명령에서 수행할 작업을 결정합니다. 이 예에서 등록 터미널 pem은 CSR(Certificate Signing Request)이 Base64 PEM 형식의 텍스트로 터미널에 출력됨을 나타냅니다. 등록 셀프 서명과 같은 다른 옵션을 사용하여 자체 서명 인증서를 생성하거나, HTTP URL을 정의하고 SCEP(Simple Certificate Enrollment Protocol) 프로토콜을 활용하도록 등록 URL을 구성할 수 있습니다. 이 두 가지 방법은 모두 이 문서의 범위를 벗어납니다.
일련 번호 없음	IOS XE 디바이스 직렬을 CSR에 추가할지 여부를 결정합니다. 이렇게 하면 crypto pki enroll 명령 중에 프롬프트가 비활성화됩니다.
fqdn 없음	FQDN(정규화된 도메인 이름)을 CSR에 추가할지 여부를 결정합니다. 이렇게 하면 crypto pki enroll 명령 중에 프롬프트가 비활성화됩니다.
ip 주소 없음	IOS XE 디바이스 IP 주소를 CSR에 추가할지 여부를 결정합니다. 이렇게 하면 crypto pki enroll 명령 중에 프롬프트가 비활성화됩니다.
주체 이름 cn=router.example.cisco.com	CSR에 추가될 X500 형식을 나타냅니다.
subject-alt-name myrouter.example.cisco.com을 참조하십시오.	IOS XE 17.9.1부터 쉼표로 구분된 주체 대체 이름(SAN) 값 목록을 CSR에 추가할 수 있습니다.
revocation-check 없음	IOS XE 디바이스에서 인증서의 유효성을 확인하는 방법을 나타냅니다. CRL(Certificate Revocation List), OCSP(Online Certificate Status Protocol)와 같은 옵션은 선택한 Certificate Authority에서 지원하는 경우 사용할 수 있습니다. 이는 주로 구성된 다른 IOS XE 기능 또는 서비스에서 신뢰 지점을 사용할 때 사용됩니다. 인증서가 신뢰 지점으로 인증될 경우에도 폐기 상태

	가 확인됩니다.
rsakeypair rsaKey	이 특정 레이블과 함께 RSA 키 쌍을 활용하도록 명령에 지시합니다. ECDSA 인증서의 경우 EC 키의 레이블을 참조하는 "eckeypair ecKey" 명령을 사용합니다
해시 sha256	이 명령은 사용할 해싱 알고리즘의 유형에 영향을 줍니다. 옵션은 SHA1, SHA256, SHA384, SHA512입니다

crypto pki 등록

crypto pki enroll 명령은 지정된 신뢰 지점에서 enrollment 명령을 트리거하는 데 사용됩니다. (명령 구문)
예를 들어, 이전에 trustpoint에 표시된 crypto pki enroll labTrustpoint 명령은 아래 예와 같이 Base64 PEM 텍스트 형식으로 터미널에 CSR(Certificate Signing Request)을 표시합니다.

이제 이 인증서 서명 요청을 텍스트 파일로 저장하거나, 명령줄에서 복사하여 붙여넣을 수 있습니다. 이는 서드파티 CA에 검증 및 서명을 제공하기 위한 목적입니다.

<#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---
```

crypto pki 인증

crypto pki authenticate 명령은 신뢰할 수 있는 CA 인증서를 지정된 신뢰 지점에 추가하는 데 사용됩니다. 각 신뢰 지점은 한 번에 인증할 수 있습니다. 즉, 신뢰 지점은 단일 CA 루트 또는 중간 인증

서만 포함할 수 있습니다. 명령을 두 번 실행하고 새 인증서를 추가하면 첫 번째 인증서를 덮어쓰게 됩니다.

명령 등록 터미널 pem이 구성된 경우 crypto pki authenticate 명령은 라우터에 Base64 PEM 형식의 인증서를 CLI를 통해 업로드하도록 요청합니다(명령 구문).

관리자는 나중에 디바이스의 ID 인증서를 가져올 목적으로 인증서 체인에 루트 및 선택적 중간 인증서를 추가하기 위해 신뢰 지점을 인증할 수 있습니다.

관리자는 또한 신뢰 지점을 인증하여 다른 신뢰할 수 있는 루트 CA를 IOS XE 디바이스에 추가하여 해당 피어 디바이스와의 프로토콜 핸드셰이크 중에 피어 디바이스와의 신뢰 관계를 활성화할 수 있습니다.

추가 설명을 위해, 피어 디바이스는 "루트 CA 1"에 의해 서명된 인증서 체인을 특징으로 할 수 있다. IOS XE 디바이스와 피어 디바이스 간의 프로토콜 핸드셰이크 중에 인증서 검증이 성공하려면 관리자는 crypto pki authenticate 명령을 사용하여 IOS XE 디바이스의 신뢰 지점에 CA 인증서를 추가할 수 있습니다.

기억해야 할 주요 항목: crypto pki authenticate를 사용하여 신뢰 지점을 인증하는 것은 항상 ID 인증서를 추가하는 것이 아니라 CA 루트 또는 중간 인증서를 신뢰 지점에 추가하는 것입니다. 이 개념은 다른 피어 디바이스에서 자체 서명 인증서를 인증하는 데에도 적용됩니다.

아래 예에서는 crypto pki authenticate 명령을 사용하여 이전 신뢰 지점을 인증하는 방법을 보여줍니다.

<#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
```

crypto pki 가져오기

이 명령은 ID(ID) 인증서를 신뢰 지점으로 가져오는 데 사용됩니다. 단일 신뢰 지점은 단일 ID 인증

서만 포함할 수 있으며, 명령을 두 번째로 실행하면 이전에 가져온 인증서를 덮어쓰라는 프롬프트가 표시됩니다. (명령 구문)

아래 예에서는 crypto pki import 명령을 사용하여 이전 신뢰 지점에서 ID 인증서를 예제 신뢰 지점으로 가져오는 방법을 보여줍니다.

```
<#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
```

신뢰 지점에서 이 인증서를 직접 서명하는 데 사용되는 CA 인증서를 인증하기 전에 인증서를 가져오려고 하면 관리자가 오류를 수신하게 됩니다.

```
<#root>

Router(config)#

crypto pki import labTrustpoint certificate

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

피어 CA 인증서 인증

피어 CA 인증서는 CA 인증서를 추가하는 것과 동일한 방법을 사용하여 IOS XE에 추가됩니다. 즉, crypto pki authenticate 명령을 사용하여 신뢰 지점에 대해 인증됩니다.

아래 명령은 신뢰 지점을 생성하고 피어 서드파티 CA 인증서를 인증하는 방법을 보여줍니다.

1. 먼저 피어 CA 인증서를 보유할 몇 가지 설명 이름으로 신뢰 지점을 생성합니다
2. crypto pki authenticate 명령이 명령줄을 통해 인증서를 요청하도록 등록 터미널 pem을 구성합니다.
3. 가져오기 프로세스에서 CRL/OCSP 검사를 건너뛰려면 revocation-check none을 구성합니다
4. 신뢰 지점을 인증하고 인증서를 제공합니다.
5. 피어 CA 인증서에 필요한 대로 1~4단계를 반복합니다(신뢰 지점당 CA 인증서 하나만 기억하십시오!).

<#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
```

하나 이상의 중간 인증서 인증

앞의 예에서는 crypto pki enroll을 사용하여 CSR을 생성하고, crypto pki authenticate를 사용하여 루트 CA 인증서를 인증한 다음 crypto pki import를 사용하여 ID 인증서를 가져오는 방법을 자세히 설명합니다.
그러나 중간 인증서를 도입할 때는 프로세스가 약간 다릅니다. 두려워 말라, 동일한 개념과 명령이 여전히 적용! 차이점은 인증서를 보유하는 신뢰 지점이 배치되는 방법에 있습니다.

각 신뢰 지점은 단일 루트 또는 중간 CA 인증서만 포함할 수 있습니다. 따라서 아래에 표시된 것과 같은 CA 체인이 있는 예에서는 crypto pki authenticate 명령을 사용하여 둘 이상의 CA 인증서를 추가할 수 없습니다.

<#root>

- Root CA

 - Intermediate CA 1

- Identity Certificate

해결책:

1. 인증된 루트 CA를 보유할 신뢰 지점을 생성합니다.
2. 그런 다음 CSR을 생성하는 데 사용되는 신뢰 지점을 사용하여 중간 인증서를 인증합니다
3. 마지막으로 ID 인증서를 최종 신뢰 지점으로 가져옵니다.

아래 표를 사용하면 이전 체인에 해당하는 색상으로 신뢰 지점 매핑을 명령하여 시각화를 지원하는 인증서를 예시할 수 있습니다.

인증서 이름	사용할 신뢰 지점	사용할 명령
루트 CA	crypto pki trustpoint ROOT-CA	crypto pki authenticate ROOT-CA
중간 CA 1	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint(암호화 pki labTrustpoint 인증)
ID 인증서	crypto pki trustpoint labTrustpoint 다운로드	crypto pki import labTrustpoint certificate

동일한 논리를 두 개의 중간 CA 인증서가 있는 인증서 체인에 적용할 수 있습니다. 새로운 중간 CA가 IOS XE 컨피그레이션에 적용되는 위치를 시각화하는 데 도움이 되도록 색상이 다시 제공됩니다.

<#root>

- Root CA

- Intermediate CA 1

- Intermediate CA 2

- Identity Certificate

인증서 이름	사용할 신뢰 지점	사용할 명령
루트 CA	crypto pki trustpoint ROOT-CA	crypto pki authenticate ROOT-CA
중간 CA 1	crypto pki trustpoint INTER-CA	crypto pki INTER-CA 인증

중간 CA 2	crypto pki trustpoint labTrustpoint 다운로드	crypto pki authenticate labTrustpoint(암호화 pki labTrustpoint 인증)
ID 인증서	crypto pki trustpoint labTrustpoint 다운로드	crypto pki import labTrustpoint certificate

자세히 보면 다음과 같은 두 가지 패턴을 볼 수 있습니다.

1. 모든 루트 또는 중간 인증서는 crypto pki authenticate(개수에 관계없이)를 사용하여 신뢰 지점에 로드됩니다.
2. 또한 디바이스의 ID 인증서(ID 인증서를 직접 서명한 인증서 읽기) 이전의 최종 인증서가 ID 인증서를 가져올 동일한 신뢰 지점에서 항상 인증된다는 것을 알 수 있습니다.
    - 앞에서 설명한 오류와 마찬가지로, IOS XE에서는 관리자가 이 인증서를 직접 서명하는 데 사용된 CA 인증서를 먼저 인증하지 않고 인증서를 가져올 수 없습니다.

대부분의 구축에서 관리자가 인증서 체인에 2개 이상의 중간 CA를 볼 수 있지만 위의 두 패턴은 2개를 초과하는 중간 인증서에 얼마든지 사용할 수 있습니다.

완전성을 위해 다음 루트/ID 인증서 테이블도 제공됩니다.

<#root>

```
- Root CA
```

```
 - Identity Certificate
```

인증서 이름	사용할 신뢰 지점	사용할 명령
루트 CA	crypto pki trustpoint labTrustpoint 다운로드	crypto pki authenticate labTrustpoint(암호화 pki labTrustpoint 인증)
ID 인증서	crypto pki trustpoint labTrustpoint 다운로드	crypto pki import labTrustpoint certificate

확인

- 인증 또는 가져오기 프로세스 중에 IOS XE에서 다양한 온전성 검사를 수행하여 인증서가 유효하고 올바른 형식인지 확인합니다. 이러한 오류는 화면에 인쇄되거나 로그(로깅 표시)에서 "CRYPTO_PKI"로 시작하는 행을 찾습니다.

다음은 몇 가지 일반적인 예입니다.

유효한 Before/After 검사는 구성된 시간과 인증서에 있는 시간을 기준으로 수행됩니다

<#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
```

revocation-check가 비활성화된 경우 IOS XE는 인증서를 가져오기 전에 구성된 방법을 통해 폐기 검사를 수행합니다

```
<#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
```

인증 또는 가져온 신뢰 지점 컨피그레이션에 대한 세부 정보를 보려면 다음 명령을 사용하십시오.

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

문제 해결

가져오기 문제 또는 기타 PKI 문제를 디버깅할 때 다음 디버그를 활용합니다.

```
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
```

고급 IOS PKI 개념

PKCS12 형식의 인증서 가져오기

일부 CA 공급자는 PKCS#12 형식(.pfx, .p12)으로 파일을 다시 제공할 수 있습니다.

PKCS#12는 루트 인증서에서 ID 인증서를 통한 전체 인증서 체인이 rsa 키 쌍과 함께 번들로 제공되는 특수한 유형의 인증서 형식입니다.

이 형식은 IOS XE로 가져올 때 매우 편리하며 아래 명령을 사용하여 쉽게 가져올 수 있습니다.

```
<#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.
```

PKCS12 또는 PEM 인증서 내보내기

관리자는 인증서를 터미널에 Base64 일반 텍스트 PEM, Base64 암호화된 일반 텍스트 또는 PKCS12 형식으로 내보내 다른 피어 디바이스로 가져올 수 있습니다.

이 기능은 새 피어 디바이스를 가져올 때 유용합니다. 관리자가 디바이스 ID 인증서에 서명한 루트 CA 인증서를 공유해야 합니다.

일부 샘플 구문은 다음과 같습니다.

```
<#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
```

RSA 키 내보내기

다른 디바이스로 가져오거나 트러블슈팅 작업에 사용하기 위해 RSA 키를 내보내야 할 수도 있습니다. 키 쌍이 내보낼 수 있는 것으로 생성되었다고 가정하면 암호화 방법(DES, 3DES, AES) 및 비밀번호와 함께 crypto key export 명령을 사용하여 키를 내보낼 수 있습니다.

샘플 사용:

<#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-----
```

키를 내보낼 수 없는 경우 오류가 표시됩니다.

<#root>

```
Router(config)#
crypto key export rsa kydavis.cisco.com pem terminal 3des mySecretPassword

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

오프박스(off-box)에서 생성된 RSA 키 가져오기

일부 관리자는 RSA 및 인증서 생성을 오프박스로 수행할 수 있으며, 비밀번호를 사용하여 아래와

같이 crypto key import 명령을 사용하여 RSA 키를 가져올 수 있습니다.

<#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.
```

RSA 키 삭제

crypto key zeroize rsaKey 명령을 사용하여 rsaKey라는 RSA 키 쌍을 삭제합니다.

신뢰 풀을 통해 Cisco Trusted CA 번들 가져오기

신뢰 풀은 신뢰 지점마다 약간씩 다르지만 코어 사용량은 동일합니다. 일반적으로 신뢰 지점에는 단일 CA 인증서가 포함되며 신뢰 풀에는 다수의 신뢰받는 CA가 포함됩니다.

Cisco는 https://www.cisco.com/security/pki/에서 CA 번들을 게시합니다.

한 가지 일반적인 용도는 아래 명령을 사용하여 ios_core.p7b 파일을 다운로드하는 것입니다.

<#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)#
```

자주 묻는 질문(FAQ)

신뢰 지점을 삭제하면 지정된 CSR에서 부여된 CSR 또는 인증서 체인이 무효화됩니까?

아니요. CSR이 생성되어 저장되면 CSR을 무효화하지 않고 신뢰 지점을 삭제하고 다시 추가할 수 있습니다.

Cisco 기술 지원 부서에서는 인증서를 인증/가져오는 작업이 잘못되었을 때 이를 새로 시작하는 데 자주 사용합니다.

관리자 또는 지원 엔지니어가 RSA 키를 다시 생성하지 않는 한, CSR 또는 서명된 인증서 체인을 가져올 수 있습니다.

중요! 신뢰 지점을 제거하면 일부 서비스나 기능에서 해당 인증서를 현재 사용 중인 경우 더 문제가 될 수 있는 모든 인증/가져온 인증서가 삭제됩니다.

신뢰 지점에 CSR을 생성하면 기존 인증서가 무효화됩니까?

아니요. 이는 인증서가 곧 만료될 때 일반적입니다. 관리자는 crypto pki enroll 명령을 수행하여 새 CSR을 생성하고 인증/가져온 기존 인증서가 계속 사용 중인 동안 CA와의 인증서 서명 프로세스를 시작할 수 있습니다. 관리자가 인증서를 crypto pki authenticate/crypto pki import로 교체하는 순간은 기존 인증서가 교체되는 순간입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.