IOS XE PKIを使用したCA署名付き証明書の設定

内容

はじめに

このドキュメントは、サードパーティの認証局(CA)によって署名されたIOS XE証明書を設定するための一般的なガイドです。

このドキュメントでは、デバイスがID(Identity)証明書として機能するようにマルチレベルCA署名付きチェーンをインポートする方法と、証明書の検証のために他のサードパーティ証明書をインポートする方法の両方について説明します。

前提条件

要件

IOS PKI機能を使用する場合は、NTPとクロック時間を設定する必要があります。

管理者がNTPを設定していない場合、将来/過去の日付/時刻で生成される証明書に問題がある可能性があります。この日付や時間のずれは、インポートの問題やその他の問題を引き起こす可能性があります。

NTPの設定例：

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

使用するコンポーネント

- Cisco IOS® XE17.11.1aを実行しているCiscoルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントに記載されている機能の中には、古いIOS XEバージョンでは使用できないものもあります。可能であれば、コマンドや機能が導入または変更された際に注意を払って文書化してください。

特定のバージョンのIOS XE PKI機能の公式ドキュメントを常に参照して、特定のバージョンに関連する制限や変更を理解してください。

例:

- 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の設定

IOS XE PKI証明書を使用する場合、管理者は次のアクションを実行する必要があります。

1. 機能またはサービスで使用するキーを作成します(crypto key generate)。

2. さまざまなパラメータを使用してトラストポイントを設定し、キーをリンクします。(crypto pki trustpoint)
3. 証明書署名要求(CSR)の生成(crypto pki enroll)
4. 署名用のCSRをCAに提供します(このドキュメントでは説明しません)。
5. ルートおよび中間CA証明書の認証(crypto pki authenticate)
6. デバイス証明書のインポート(crypto pki import)
7. オプション：ピアCA証明書を認証する(crypto pki authenticate)

これらの手順については、以降のセクションで、特定のアクションに必要なコマンド別にグループ化して詳しく説明します。

暗号キー生成

多くの管理者は、ルータでSecure Socket Shell(SSH)を有効にするために、または機能の設定ガイドの一部として、このコマンドを入力しています。しかし、コマンドが実際に行っていることを解剖していない人はほとんどいません。

たとえば、次のコマンドを使用します。

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

これらのコマンドを特定の部分に分割すると、使用方法の詳細が表示されます。

- 黒（暗号キー生成）のコマンドの最初の部分は、新しいキーを作成することをルータに指示します。暗号キーのエクスポート、暗号キーのインポート、暗号キーのゼロサイズなど、その他のオプションもあります。これらについては後で詳しく説明します。
- 緑色(rsa general-keys、ec)のコマンドの次の部分は、作成するキーのタイプを正確にルータに指示します。ほとんどの場合、公開/秘密キーで構成されるRivest-Shamir-Adleman(RSA)キーペアが使用されますが、管理者は、ECDSA証明書を必要とする機能やECDHEハンドシェイクで使用する楕円曲線(EC)を設定することもできます。
- orangeのコマンドは、キーのサイズを定義します。
    - RSAでは、モジュラスは用語であり、512 ~ 4096などの値を使用できます。デフォルトのモジュールサイズはバージョンによって異なりますが、次世代暗号化に関するシスコのベストプラクティスに従い、2048より大きいキーを使用することを推奨します。
    - ECの場合、key-sizeコマンドでキーのビット数を指定する必要があります。オプションは、256、384、または512です。
- purpleのコマンドは、このキーのラベルを定義します。管理者は同じIOS XEデバイス上でさまざまな目的のために複数のキーを定義する必要がある場合があるため、これは重要です。ラベルは、特定の機能で使用する正確なキーを指定するために使用されます。可能であれば、常にラベルを使用して使用中のキーを区別し、フィーチャへのキーの割り当てを容易にします。たとえば、ラベルSSH、ラベルCUBE、ラベルHTTPSは、異なるサービスまたは機能で使用する2つのキーを作成します。
    - キーのデフォルトラベルは、デバイスのhostname.domainです。一部のデバイスでは

、初回起動時にRSAキーが生成される場合があります。ラベルのポストフィックスを入力しないと、管理者が誤って誤ったキーを上書きまたは再生成する危険性があります

- 青で示した最後のコマンドは、エクスポート可能なポストフィックスです。このコマンドでは、キーをcrypto pki exportコマンドで使用してエクスポートしたり、他のシステムで使用したりできることが詳しく説明されています。たとえば、ピアのハイアベイラビリティデバイスにインポートして、HAペアの両方のメンバーが1つのキーを使用するようにしたり、WiresharkなどのトラブルシューティングツールでRSAベースのTLSセッションを復号化するために使用したりする場合があります。RSAキーは最初からエクスポート可能としてのみ作成できることを述べなければならない理由は何であれ。管理者がエクスポート不可能なRSAキーを作成した場合、このキーはキーを再生成しない限りエクスポート可能に設定できません。この場合、そのキーを使用して作成されたすべての証明書を無効にするなど、他の機能に波紋が生じる可能性があります。つまり、crypto key move rsaKeyLabel non-exportableコマンドを使用すると、キーを再生成せずにエクスポート可能なキーをエクスポート不可能なキーにダウングレードできます

設定例:

<#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
```

検証例：

<#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
```

クリプトPKIトラストポイント

トラストポイントは、IOS XE内でPKI証明書を保存および管理するための「フォルダのような」概念です(コマンド構文)。

大まかに見ると、

1. 各IOS XEトラストポイントには、crypto pki authenticateコマンドを使用してロードされた単一のルートまたは中間CA証明書を含めることができます。認証されたトラストポイントは、現在デバイスによって信頼されている証明書を追加するものと考えてください。
2. 各IOS XEトラストポイントは、crypto pki importコマンドを使用してロードされた単一のID(ID)証明書をインポートすることもできます。ID証明書はこのデバイス証明書で、通常は一部のサービスまたは機能に関連付けられています。
3. 管理者は、同じトラストポイントでauthenticateコマンドとimportコマンドを使用できます（このコマンドは、後述するID証明書をインポートするために必要です）。認証/インポートワークフローを使用する場合、トラストポイントには2つの証明書（ルート/中間+アイデンティティ証明書）が含まれます。
4. 信頼されたピアのルート/中間CA証明書を保存する目的でトラストポイントを使用する場合、 crypto pki認証 コマンドが必要です。このシナリオでは、トラストポイントには、管理者によって認証された1つの証明書だけが含まれます。

注：crypto pki authenticateとcrypto pki importに関する以降のセクション、およびマルチレベル証明書の認証/インポートの例について詳しく説明した以降のセクションでは、これら4つの箇条書きについて詳しく説明します。

トラストポイントには、さまざまなコマンドを設定できます。これらのコマンドは、トラストポイントでcrypto pki enrollコマンドを使用してデバイスによって作成される証明書署名要求(CSR)内の値に影響を与えます。

トラストポイントで使用できるコマンドは数多くあります（このドキュメントでは非常に多く、詳細を説明できません）が、一般的な例については次のトラストポイントの例と表の両方で説明しています。

```
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
```

コマンド	説明
crypto pkiトラストポイントlabTrustpoint	このトラストポイントの人間が読める設定ラベル。後のコマンドで機能またはサービスにリンクするために使用します。
enrollment terminal pem	crypto pki enrollコマンドが実行するアクションを決定します。 この例では、enrollment terminal pemは、証明書署名要求(CSR)がBase64 PEM形式のテキストで端末に出力されることを示しています。 enrollment selfsignedなどのその他のオプションを使用して自己署名証明書を作成したり、enrollment urlを設定してHTTP URLを定義したり、Simple Certificate Enrollment Protocol(SCEP)プロトコルを利用したりできます。これらの方法はどちらも、このドキュメントの範囲外です。
シリアル番号なし	IOS XEデバイスシリアルがCSRに追加されるかどうかを決定します。これにより、crypto pki enrollコマンド中のプロンプトも無効になります。
fqdnなし	完全修飾ドメイン名(FQDN)をCSRに追加するかどうかを決定します。これにより、crypto pki enrollコマンド中のプロンプトも無効になります。
IPアドレスなし	IOS XEデバイスのIPアドレスをCSRに追加するかどうかを決定します。これにより、crypto pki enrollコマンド中のプロンプトも無効になります。
subject-name cn=router.example.cisco.com	CSRに追加されるX500形式を示します。

subject-alt-name myrouter.example.cisco.com	IOS XE 17.9.1以降では、サブジェクト代替名(SAN)値のカンマ区切りリストをCSRに追加できます。
revocation-check none	IOS XEデバイスが証明書の有効性を確認する方法を示します。Certificate Revocation List（CRL；証明書失効リスト）、Online Certificate Status Protocol（OCSP；オンライン証明書ステータスプロトコル）などのオプションは、選択した認証局でサポートされている場合に使用できます。これは主に、トラストポイントが他の設定済みIOS XE機能またはサービスによって使用される場合に使用されます。証明書がトラストポイントで認証される場合も、失効ステータスがチェックされます。
rsakeypair rsaKey	この特定のラベルでRSAキーペアを使用するようにコマンドに指示します。 ECDSA証明書では、ECキーのラベルを参照するコマンド「eckeypair ecKey」を使用します。
ハッシュsha256	このコマンドは、使用するハッシュアルゴリズムのタイプに影響します。オプションはSHA1、SHA256、SHA384、SHA512です

クリプトPKI登録

crypto pki enrollコマンドは、特定のトラストポイントでenrollmentコマンドをトリガーするために使用されます。(コマンド構文)
以前に表示したトラストポイントの例では、コマンドcrypto pki enroll labTrustpointを使用すると、次の例に示すように、証明書署名要求(CSR)がBase64 PEMテキスト形式で端末に表示されます。

この証明書署名要求をテキストファイルに保存したり、コマンドラインからコピーして貼り付けたりして、サードパーティCAに検証と署名を提供することができます。

<#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認証

crypto pki authenticateコマンドは、特定のトラストポイントに信頼できるCA証明書を追加するために使用されます。各トラストポイントは、一度に認証できます。つまり、トラストポイントに含めることができるCAルート証明書または中間証明書は1つだけです。このコマンドを2回実行して新しい証明書を追加すると、最初の証明書が上書きされます。

enrollment terminal pemコマンドが設定されていると、crypto pki authenticateコマンドにより、CLIを介してアップロードされるBase64 PEM形式の証明書の入力をルータが求められます(コマンド構文)。

管理者は、デバイスのID証明書を後でインポートする目的で、証明書チェーンにルート証明書とオプションの中間証明書を追加するためにトラストポイントを認証できます。

また、管理者は、ピアデバイスとのプロトコルハンドシェイク中にピアデバイスとの信頼関係を有効にするために、トラストポイントを認証してその他の信頼されたルートCAをIOS XEデバイスに追加することもできます。

さらに詳しく説明するために、ピアデバイスは「ルートCA 1」によって署名された証明書チェーンを備えている場合があります。IOS XEデバイスとピアデバイス間のプロトコルハンドシェイク中の証明書検証を成功させるには、管理者はcrypto pki authenticateコマンドを使用して、IOS XEデバイスのトラストポイントにCA証明書を追加できます。

覚えておくべき主な項目：crypto pki authenticateを使用したトラストポイントの認証は、常にCAルート証明書または中間証明書をトラストポイントに追加するためのものであり、ID証明書を追加するためのものではありません。この概念は、別のピアデバイスからの自己署名証明書の認証にも適用されます。

次の例は、crypto pki authenticateコマンドを使用して、以前のトラストポイントを認証する方法を示しています。

<#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
```

暗号化PKIインポート

このコマンドは、ID(ID)証明書をトラストポイントにインポートするために使用されます。単一のトラストポイントには単一のID証明書のみを含めることができ、このコマンドを2回発行すると、以前にインポートした証明書を上書きするように求められます。 (コマンド構文)

次の例は、crypto pki importコマンドを使用して、以前の例のトラストポイントにID証明書をインポートする方法を示しています。

<#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
```

トラストポイントが、この証明書に直接署名するために使用されるCA証明書を認証する前に、証明書をインポートしようとすると、管理者は工ラーを受け取ります。

<#root>

```
Router(config)#

crypto pki import labTrustpoint certificate

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

ピアCA証明書の認証

ピアCA証明書は、CA証明書を追加するのと同じ方法でIOS XEに追加されます。つまり、crypto pki authenticateコマンドを使用して、トラストポイントに対して認証されます。

次のコマンドは、トラストポイントを作成し、ピアのサードパーティCA証明書を認証する方法を示しています。

1. 最初に、ピアCA証明書を保持する、わかりやすい名前を付けてトラストポイントを作成します
2. crypto pki authenticateコマンドがコマンドラインで証明書を要求するように、enrollment terminal pemを設定します。
3. インポートプロセス中にCRL/OCSPチェックをスキップするようにrevocation-check noneを設定します
4. トラストポイントを認証し、証明書を提供します
5. ピアCA証明書に必要に応じて、手順1 ~ 4を繰り返します（トラストポイントごとに1つのCA証明書のみを記憶してください）。

<#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
```

1つ以上の中間証明書の認証

前述の例では、crypto pki enrollを使用してCSRを生成し、crypto pki authenticateを使用してルートCA証明書を認証し、その後crypto pki importを使用してID証明書をインポートする方法を詳しく説明しています。
ただし、中間証明書を導入する場合、プロセスは若干異なります。心配しないでください。同じ概念とコマンドが適用されます。違いは、証明書を保持するトラストポイントのレイアウトにあります。

各トラストポイントに含めることができるルートCA証明書または中間CA証明書は1つだけであることに注意してください。そのため、次に示すようなCAチェーンがある例では、crypto pki authenticateコマンドを使用して複数のCA証明書を追加することはできません。

<#root>

```
- Root CA


 - Intermediate CA 1


   - Identity Certificate
```

ソリューション：

1. 認証されたルートCAを保持するトラストポイントを作成します。
2. 次に、CSRの作成に使用したトラストポイントで中間証明書を認証します
3. 最後に、最終的なトラストポイントにID証明書をインポートします。

次の表を使用して、可視化を支援する前のチェーンに対応する色を使用したトラストポイントマッピングに対する証明書のコマンドを示すことができます。

証明書名	使用するトラストポイント	使用するコマンド
ルートCA	crypto pkiトラストポイント ルートCA	crypto pki authenticate ROOT-CA
中間CA 1	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint
アイデンティティ証明書	crypto pkiトラストポイント labTrustpoint	crypto pki import labTrustpoint 証明書

2つの中間CA証明書を持つ証明書チェーンにも同じロジックを適用できます。ここでも、新しい中間CAがIOS XE設定に適用される場所を視覚化するのに役立つ色が提供されます。

<#root>

- Root CA

 - Intermediate CA 1

 - Intermediate CA 2

 - Identity Certificate

証明書名	使用するトラストポイント	使用するコマンド
ルートCA	crypto pkiトラストポイントルートCA	crypto pki authenticate ROOT-CA
中間CA 1	crypto pki trustpoint CA間	crypto pki authenticate INTER-CA
中間CA 2	crypto pkiトラストポイントlabTrustpoint	crypto pki authenticate labTrustpoint
アイデンティティ証明書	crypto pkiトラストポイントlabTrustpoint	crypto pki import labTrustpoint 証明書

よく見ると、次の2つのパターンに気付きます。

1. すべてのルート証明書または中間証明書は、crypto pki authenticateを使用して（いくつあるかにかかわらず）トラストポイントにロードされます。
2. また、デバイスのID証明書（ID証明書に直接署名したもの）の前にある最終的な証明書は、ID証明書のインポート先となる同じトラストポイントで常に認証されます。
    - 前述のエラーと同様に、IOS XEでは、最初に、この証明書に直接署名するために使用されるCA証明書を認証しない限り、管理者は証明書をインポートできません。

上記の2つのパターンは、2つを超える任意の数の中間証明書に使用できますが、ほとんどの場合、管理者は証明書チェーンに3つ以上の中間CAを確認できます。

完全を期すために、次のルート/ID証明書テーブルも提供されています。

<#root>

- Root CA

 - Identity Certificate

証明書名	使用するトラストポイ	使用するコマンド

	ント	
ルートCA	crypto pkiトラストポイントlabTrustpoint	crypto pki authenticate labTrustpoint
アイデンティティ証明書	crypto pkiトラストポイントlabTrustpoint	crypto pki import labTrustpoint 証明書

検証

- 認証またはインポートプロセス中に、証明書が有効で適切な形式であることを確認するために、IOS XEによってさまざまな健全性チェックが実行されます。これらのエラーが画面に表示されるか、ログ(show logging)で「CRYPTO_PKI」で始まる行が検索されます。

一般的な例をいくつか次に示します。

有効なBefore/Afterチェックは、証明書で検出された設定時刻と比較して実行されます

```
<#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-checkが無効になっていない場合、IOS XEは証明書をインポートする前に、設定済みの方式でrevocation-checkを実行します

```
<#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
```

トラストポイント設定、認証済み、またはインポート済みの詳細を表示するには、次のコマンドを使用します。

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

（「トラブルシューティング」）

インポートの問題やその他のPKIの問題をデバッグする場合は、次のデバッグを使用します。

```
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
```

高度なIOS PKIの概念

PKCS12形式の証明書のインポート

一部のCAプロバイダーは、PKCS#12形式(.pfx、.p12)でファイルを提供することがあります。

PKCS#12は、ルート証明書からID証明書までの証明書チェーン全体がrsaキーペアと一緒にバンドルされる、特殊なタイプの証明書形式です。

この形式は、IOS XEでのインポートに非常に便利で、次のコマンドを使用して簡単にインポートできます。

<#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またはPEM証明書のエクスポート

管理者は、証明書をBase64プレーンテキストPEM、Base64暗号化プレーンテキスト、またはPKCS12形式で端末にエクスポートして、他のピアデバイスにインポートできます。

これは、新しいピアデバイスを起動し、管理者がデバイスID証明書に署名したルートCA証明書を共有する必要がある場合に便利です。

次に構文の例をいくつか示します。

<#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キーのエクスポート

他のデバイスにインポートしたり、トラブルシューティング作業で使用したりするために、RSAキーをエクスポートする必要がある場合があります。キーペアがエクスポート可能な形式で作成されていると仮定した場合、暗号方式(DES、3DES、AES)およびパスワードとともにcrypto key exportコマンドを使用してキーをエクスポートできます。

使用例：

<#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-----
```

キーがエクスポート可能でない場合は、エラーが表示されます。

```
<#root>

Router(config)#

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


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

オフボックスで生成されたRSAキーのインポート

一部の管理者はRSAおよび証明書の作成をオフボックスで実行できます。次に示すように、パスワードを使用してcrypto key importコマンドを使用してRSAキーをインポートできます。

```
<#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キーの削除

コマンドcrypto key zeroize rsa rsaKeyを使用して、rsaKeyという名前のRSAキーペアを削除しま

す。

Trustpoolを使用したCisco Trusted CAバンドルのインポート

トラストプールはトラストポイントとはわずかに異なりますが、コアの使用率は同じです。トラストポイントには通常1つのCA証明書が含まれ、トラストプールには多数の信頼できるCAが含まれます。

シスコはhttps://www.cisco.com/security/pki/でCAバンドルを公開しています。

一般的な使用方法の1つは、次のコマンドを使用してios_core.p7bファイルをダウンロードすることです。

<#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)#
```

よく寄せられる質問（FAQ）

トラストポイントを削除すると、CSRまたは特定のCSRから付与された証明書チェーンが無効になりますか。

いいえ。CSRが生成されて保存されると、CSRを無効にせずにトラストポイントを削除して再度追加できます。

これは、証明書の認証/インポートが失敗した場合に新たに開始するために、シスコテクニカルサポートでよく使用されます。

管理者またはサポートエンジニアがRSAキーを再生成しない限り、CSRまたは署名付き証明書チェーンをインポートして認証またはインポートできます。

重要：トラストポイントを削除すると、認証またはインポートされた証明書が削除されます。これらの証明書が現在あるサービスまたは機能で使用されていると仮定すると、問題が生じる可能性が高くなります。

トラストポイントでCSRを生成すると、既存の証明書が無効になりますか。

いいえ。これは、証明書の有効期限が近づいている場合に一般的です。管理者は、crypto pki enrollコマンドを実行して、認証またはインポートされた既存の証明書が使用されている間に、新しいCSRを作成し、CAを使用して証明書署名プロセスを開始できます。管理者が証明書をcrypto pki authenticate/crypto pki importで置き換えた瞬間に、古い証明書が置き換えられます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。